6-Month CCNA 200-301 Study Plan for Aspiring Network Engineers

Welcome to your CCNA journey! This comprehensive 6-month plan is designed for a complete beginner to become a proficient network engineer and **ace the Cisco CCNA 200-301 exam on the first attempt**. The plan balances theory, hands-on practice, and regular review, with ~10–15 hours per week (roughly 2 hours/day for 5–6 days, allowing rest days [1]). Each month is divided into 4 weeks, each with clear objectives, curated resources (free options whenever possible), time allocations, and checkpoints. We'll cover **all CCNA exam blueprint domains** – Network Fundamentals, Network Access, IP Connectivity, IP Services, Security Fundamentals, Automation & Programmability – **and list every subtopic** so nothing is missed. We'll also integrate broader networking skills (troubleshooting, design, Linux basics, Python for automation, documentation) to shape you into a well-rounded network engineer.

Exam Blueprint Coverage: *The CCNA 200-301 exam* (120 minutes, ~90–110 questions [2], passing ~825/1000) covers six domains [3]: **Network Fundamentals (20%)**, **Network Access (20%)**, **IP Connectivity (25%)**, **IP Services (10%)**, **Security Fundamentals (15%)**, and **Automation & Programmability (10%)**. Below is a full topic list for reference (you should be able to explain each confidently by the end [4]):

- **1.0 Network Fundamentals:** Roles and functions of network components (routers, L2/L3 switches, next-gen firewalls/IPS, access points, wireless controllers, endpoints, servers, PoE) [5]; Network topology architectures (two-tier vs three-tier, spine-leaf, WAN, SOHO, on-prem vs cloud) [6]; Physical interfaces and cabling (single-mode vs multimode fiber, copper, Ethernet shared vs point-to-point) [7]; Interface/cable issues (collisions, errors, duplex/speed mismatches); **TCP vs UDP** [8]; IPv4 addressing and **subnetting** (configure & verify) [9]; Need for private IPv4 addressing [10]; IPv6 addressing and prefixes (configure & verify) [11]; IPv6 address types (global/unique-local/link-local unicast, anycast, multicast, modified EUI-64) [12] [13]; Verify IP parameters on hosts (Windows `ipconfig`, Linux `ifconfig`/`ip` command, etc.); Wireless principles (non-overlapping Wi-Fi channels, SSID, RF, encryption); Virtualization fundamentals (virtual machines, containers, VRFs); Switching concepts (MAC address learning & aging, frame switching & flooding, MAC address table) [14].

- **2.0 Network Access:** VLANs (normal range) on multiple switches – access ports (data/voice), default VLAN, inter-VLAN connectivity [15]; Interswitch connectivity – trunking (802.1Q), native VLAN [16]; Layer 2 discovery protocols (CDP/LLDP) [17]; EtherChannel (LACP) for link aggregation [18]; Spanning Tree Protocol (Rapid PVST+) – root bridge/port, port states (forwarding/blocking), PortFast [19] [20]; Wireless architectures (Cisco centralized WLC vs autonomous AP modes); Physical WLAN components and connections; AP and WLC management access (Telnet/SSH, TACACS+/RADIUS, HTTP/HTTPS, console) [21] [22]; Use a **GUI to configure WLAN** (create SSIDs, set WPA2/WPA3 security, QoS profiles, etc.).

- **3.0 IP Connectivity:** Routing table components (routing protocol codes, prefixes, masks, next hops, AD, metrics, gateway of last resort) [23] [24]; How routers forward by default (longest prefix match, AD, metric) [25]; IPv4 and IPv6 static routing (default routes, network routes, host routes, floating static routes) [26] [27]; Single-area OSPFv2 configuration (neighbor adjacency, network types: point-to-point vs broadcast DR/BDR, router ID) [28] [29] ; Purpose and concepts of first-hop redundancy protocols (HSRP, VRRP, GLBP) for gateway redundancy [30] .

- **4.0 IP Services:** NAT (configure & verify **inside source NAT** – static NAT and NAT pools) [31] ; NTP (configure & verify in client and server mode) [32] ; DHCP and DNS (their roles in networks) [33] ; SNMP in network operations [34] ; Syslog (facilities and severity levels) [35] ; DHCP client and relay (configure & verify) [36] ; QoS concepts – *per-hop behavior (PHB)* (classification, marking, queuing, congestion management, policing, shaping) [37] ; Configure devices for remote access via SSH [38] [39] ; Functions of TFTP/FTP in networks (file transfers for configs/images) [37] [40] .

- **5.0 Security Fundamentals:** Key security concepts (threats, vulnerabilities, exploits, mitigation) [41] ; Security program elements (user awareness training, physical access controls) [42] ; Device access control (local passwords for console/VTY, timeout, login block) [43] [44] ; Password policies (complexity, rotation, multifactor auth, certificates, biometrics) [45] [46] ; IPsec VPN types (remote-access vs site-to-site) [47] [48] ; Access Control Lists (standard/extended IPv4 ACLs configuration and verification) [49] [50] ; Layer 2 security (configure DHCP snooping, Dynamic ARP Inspection, port security) [51] [52] ; AAA concepts (Authentication, Authorization, Accounting differences); Wireless security protocols (WPA, WPA2, WPA3) [53] [54] ; Configure WLAN with WPA2-PSK via GUI (e.g. on Packet Tracer wireless controller) [55] [56] .

- **6.0 Automation & Programmability:** Impact of network automation on management (centralized control, speed, reduction of human error); Traditional networks vs controller-based (Cisco DNA Center) networking [57] ; Overlay, underlay, and fabric concepts; Separation of control plane and data plane; Northbound vs southbound APIs [58] [59] ; Traditional device management vs Cisco DNA Center approach [60] ; REST API characteristics (CRUD operations, HTTP verbs, data formats like JSON) [61] [62] ; Config management tools and their capabilities (Puppet, Chef, Ansible) [63] [64] ; Interpret JSON data structures [65] [66] .

Tracking & Study Tools: Throughout this plan, we'll use tools to maximize learning: - **Note-taking & Organization:** Use a digital notebook (e.g. **Notion** or OneNote). Create a CCNA study hub to organize notes by topic and week, and track progress. One successful CCNA passer said they "downloaded OneNote for free, and used it to make notes" [67] – you can do the same with your preferred tool. We've included tips on documenting labs and making a "knowledge base" for quick review. - **Flashcards (Spaced Repetition):** Leverage **Anki** (free on Windows/Mac) to drill important facts (protocol port numbers, subnet masks, etc.). Many CCNA students create their own Anki decks [68] ; Jeremy's IT Lab even provides flashcards to complement videos [69] . We'll prompt you when to create/review flashcards. - **Lab Tools:** We'll primarily use **Cisco Packet Tracer** (free network simulator [70] – sign up on Cisco NetAcad to download). It's beginner-friendly and sufficient for CCNA labs (router/switch configs, STP, etc.). For variety or advanced practice, you can also use **GNS3** or **EVE-NG** (free emulators) with real Cisco images, or Cisco's DevNet Sandbox for hands-on with real gear (optional). - **Practice Exams/Quizzes:** Regular self-assessment is key. We recommend quality practice exams like **Boson ExSim** (paid, high-fidelity CCNA exams) and free resources like **ExamTopics** (community CCNA questions). We'll schedule quizzes and a couple of full-length mock exams in Month 6. - **Time Management & Wellness:** Consistency beats cramming. Aim for ~2 hours of focused study on weekdays and a longer block on weekends. **Take 1–2 rest days per week** [1] to avoid burnout – use them for light review or simply recharge. Each week ends with a milestone to keep you accountable. Consider **scheduling your actual CCNA exam date** toward the end of this plan – having a deadline can motivate you to stay on track [71] .

Let’s dive into the month-by-month breakdown. Each month has a theme aligned with the CCNA domains and skill progression: - **Months 1–2:** Core fundamentals – basic concepts, networking building blocks, and getting comfortable with tools. - **Months 3–4:** Intermediate configurations and protocols – switching, routing, IP services in action. - **Month 5:** Advanced topics – security and automation, tying everything together in integrated labs. - **Month 6:** Final review and exam prep – practice tests, a capstone network project, and exam readiness. - **Post-CCNA (1 Month):** Career prep – polish your resume, prepare for interviews, and plan next steps.

Throughout the plan, keep a growth mindset. **Mistakes are learning opportunities** – if a lab or concept is challenging, that’s normal! By steadily building knowledge and skills, you’ll gain confidence. Now, let’s get started on Month 1.

Month 1: Network Foundations and Basic Tools (Fundamentals Part I)

Focus: Build a strong foundation in basic networking concepts and terminology. By the end of Month 1, you should understand how networks operate at a fundamental level (OSI and TCP/IP models, what routers and switches do, basics of IP addressing) and have your study/lab environment set up. We’ll also start doing simple labs in Packet Tracer to cement concepts. **Domains covered:** Primarily *Network Fundamentals* (CCNA domain 1.0), plus basic hands-on skills.

Week 1: Introduction to Networking & Lab Setup

Objectives (Week 1):
- Grasp the **basics of computer networks** – what networks are, client/server model, the Internet structure, and common network terminology (LAN, WAN, bandwidth, latency).
- Learn about key **network components** and their roles: *routers, switches, firewalls, access points, end devices (PCs, servers)* [5] . Be able to explain how each contributes to moving data.
- Understand the **OSI 7-layer model vs TCP/IP model**, and how data flows through the layers (encapsulation/de-encapsulation). Identify which layers correspond to which devices (e.g. switch = Layer 2, router = Layer 3).
- Set up your **lab environment**: install Cisco Packet Tracer (or alternative) and familiarize with its interface. Verify you can create a simple two-node network and ping between devices.
- Establish a note-taking and study routine: create a Notion page or notebook for Week 1 notes, and set up Anki with a few starter flashcards (e.g. OSI layers, definitions of router/switch).

Resources:
- *Videos/Tutorials:*
- **“CCNA Zero-to-One: Intro to Networking”** (free YouTube, 20 min) – High-level introduction to what networks are and the components involved (search “NetworkChuck what is a network”).
- **Jeremy’s IT Lab Day 1 – Network Devices** (YouTube, ~30 min) – Covers different network device types and where they operate [72] [73] . Jeremy’s IT Lab is a free comprehensive CCNA video course (we’ll use many of his videos).
- **Cisco Networking Academy Introduction** – If enrolled in Cisco NetAcad (free), complete *Chapter 1: Networking Today* from the **Introduction to Networks v7** course (covers network components, topology examples, etc.). This provides structured content and quizzes.
- *(Optional)* **“OSI Model Explained”** by Practical Networking (YouTube, 15 min) – Excellent visualization of OSI layers and encapsulation.

- *Books/Chapters:*

- **CCNA 200-301 Official Cert Guide (Vol. 1)** by Wendell Odom – Read Chapter 1: *Networking Today* (overview of network components and basic concepts) and Chapter 2: *Networking Models* (OSI and TCP/IP models). Take notes on the purpose of each OSI layer.

- **Computer Networking: A Top-Down Approach** by Kurose & Ross – Skim Section 1.1: *What is the Internet?* and 1.3: *Network Edge and Core*. This gives a broader context of how networks are structured (nice to know, even if not directly tested).

- *Research Papers/Articles:*

- **"A Brief History of the Internet"** – (Leiner et al., 2009) – *Internet Society* article outlining how networks evolved. Read sections on the early ARPANET to appreciate why protocols and models were developed. (Good for motivation and context; not directly examinable.)
- **"OSI Model Reference Chart"** (Cisco Learning Network) – A concise chart describing all 7 OSI layers with examples [74]. Use this to quiz yourself on layer functions.

- *(Industry whitepaper)* **"Demystifying SDN for the Network Engineer"** – Cisco whitepaper introducing Software-Defined Networking in simple terms. Just read the intro to glimpse future trends (you'll revisit SDN in Month 5).

- *Online Courses:*

- **Cisco Networking Academy – Introduction to Networks (ITN) v7**: If you prefer a guided course, sign up (free) and complete *Module 1: Networking Today* and *Module 2: Basic Switch and End Device Configuration*. These include lab exercises on Packet Tracer.

- **freeCodeCamp's 4-hour Networking Basics Course** (YouTube) – If you want more lecture-style teaching on fundamentals and OSI, this video is a great supplement (covers networking basics in a beginner-friendly way).

- *Hands-On Labs/Projects:*

- **Lab 1.1: Build Your First Network** – Using Packet Tracer, create a simple network: two PCs connected by a switch. Assign IP addresses (e.g. PC1: 10.0.0.1/24, PC2: 10.0.0.2/24), and use the PT simulation mode to send a ping. Observe the encapsulation (OSI layers) in the simulation view as the ping travels [75]. *Step-by-step:* Place two PC endpoints and one switch in PT, connect via copper straight-through cables, configure IP addresses on PCs, then ping. **Expected outcome:** PCs can ping each other successfully. Document in your notes: screenshots of your Packet Tracer topology and a brief explanation of what each device/layer did to deliver the ping.
- **Lab 1.2: Exploring Packet Tracer and CLI** – In Packet Tracer, add a Cisco 2960 switch and console into it from a PC (using a console cable). Practice using the Cisco CLI: enter `show version`, `show ip interface brief`. No configuration needed, just get used to CLI navigation (we'll do more in Week 2).

- *(Mini-Project)* **Home Network Mapping:** Draw a diagram of your own home network (router, Wi-Fi AP, any devices). Identify what OSI layer each component operates at and how they connect. This personalizes concepts like modem (Layer1/2), wireless router (Layer3), etc.

- *Quizzes/Assessments:*

- **CCNA Prep Quiz – Basics (≈20 questions)**: Take a beginner quiz on network basics (try the free quiz on ExamCompass or ExamTopics' easy questions). Aim for 80%+.

- **NetAcad Chapter Quiz:** If using NetAcad, complete the Module 1 quiz to test terminology.
- Create 5 flashcards in Anki for OSI layers (e.g. “Layer 3 name?” -> “Network layer – IP addressing, routing”). Review these at week’s end, using spaced repetition.

Time Allocation (approx 12 hours):
- Videos/lectures: ~3 hours (introductions, OSI model explanations).
- Reading (Odom chapters, Kurose intro): ~2 hours.
- Labs/Hands-on: ~4 hours (Packet Tracer setup and 2 labs, including documentation).
- Quizzes/Review: ~2 hours (quiz + flashcards + reviewing notes).
- *Buffer/Break:* ~1 hour (spread as short breaks or an extra rest day if content is mastered quickly).

Milestones & Checkpoints:
- **Milestone 1:** Write a one-page summary or **blog-style note** explaining “How data moves from one computer to another over a network,” referencing the OSI model. If you can teach it simply, that’s a great sign of understanding.
- **Milestone 2:** Submit your **Lab 1.1 report** – e.g., a screenshot of your Packet Tracer network with a brief description of your ping results and what layers were involved.
- Score at least **80% on the basic networking quiz** (or identify wrong answers and clarify why).
- **Checkpoint:** Ensure Packet Tracer is working and you’re comfortable adding devices and using the simulation mode. Also verify your note-taking system (Notion/OneNote) is set up with Week 1 content neatly organized.

Motivation: Congratulations on starting! Networking might seem overwhelming at first, but remember that **every expert was once a beginner**. You’ve learned a lot of new terms this week – celebrate that. If some concepts (like OSI layers) still feel abstract, that’s okay; we will reinforce them in upcoming weeks. Take a short break before Week 2, and get ready to dive deeper.

Week 2: Network Fundamentals – Protocols and Models

Objectives (Week 2):
- Deepen your understanding of network models and protocols: specifically, know the **difference between TCP and UDP** (when to use each, characteristics like reliability vs speed) [8].
- Learn about common **protocols at each layer** (e.g. Ethernet at Layer2, IP at Layer3, TCP/UDP at Layer4, HTTP/FTP at Layer7) and how they relate to the CCNA blueprint.
- Master the concept of **encapsulation**: how data is packaged at each layer (e.g. what a “packet” vs “frame” vs “segment” is).
- Get introduced to basic device configuration: practice using Cisco IOS CLI commands for *initial switch setup* (hostname, interface descriptions, etc.) to prepare for upcoming network access topics.
- Start learning about **Cabling and Interfaces**: types of network media (fiber vs copper, Ethernet cable categories) [7] and where they are used. Identify different interface types on routers/switches in Packet Tracer.

Resources:
- *Videos/Tutorials:*
- **“TCP vs UDP”** by NetworkChuck (YouTube, 15 min) – Fun, visual comparison of TCP and UDP using analogies (e.g. phone call vs mail). Helps solidify why both exist and their pros/cons.
- **Jeremy’s IT Lab Day 3 – OSI Model & TCP/IP** (YouTube, 32 min) – Goes through encapsulation and PDUs (protocol data units) at each layer [76] [77], and specifically touches on TCP vs UDP.
- **CBT Nuggets “TCP/IP Fundamentals”** (if you have access, ~20 min) – An optional polished video on how the TCP/IP stack works, featuring real-world examples. (If no access, the above free videos suffice.)
- *(Optional)* **“How to Use Packet Tracer – Basic CLI”** (Cisco DevNet video, 10 min) – Shows how to open

the CLI in Packet Tracer and do basic config. This overlaps with NetAcad content if you are following that.

- *Books/Chapters:*
- **CCNA Official Cert Guide (Vol. 1)** – Read Chapter 3: *Protocols and Models*. Focus on sections covering TCP/IP vs OSI, encapsulation example, and a short section on TCP vs UDP. Also read Chapter 4: *Physical Layer* (to learn about cabling and media).
- **“Networking Essentials” by Cisco Press** (optional if available) – Chapter on *Networking Protocols and Communications*. It’s a lighter read reinforcing similar concepts with examples.

- Quick reference: **RFC 791 (IPv4)** and **RFC 793 (TCP)** – *Skim* the intro paragraphs of these foundational documents to see how they describe these protocols (don’t worry about deep details; this is just to experience reading an RFC).

- *Research Papers/Articles:*

- **“Understanding TCP/IP”** – an article on NetworkingAcademy.io or similar resource that explains how TCP/IP model maps to OSI layers and the role of protocols at each layer (if you have NetAcad, the course content itself is great).
- **IEEE Spectrum: “Wi-Fi & Ethernet: A History”** – A short article describing how Ethernet and Wi-Fi standards came to be. This gives insight into why certain cabling (coax, twisted-pair, fiber) and wireless channels matter.

- *(Academic)* **“End-to-End Arguments in System Design”** (Saltzer, Reed, Clark, 1984) – This seminal paper introduced the principle that reliability should be handled end-to-end (which underpins why TCP does error checking). *Optional:* Read the first 2 pages to grasp the idea behind protocols like TCP providing reliability rather than relying on network core.

- *Online Courses:*

- **Cisco NetAcad – ITN v7 Module 3: Protocols and Models** – Goes through encapsulation process with examples; includes interactive activities. Complete Packet Tracer Activity “3.5.5: Investigate the TCP/IP and OSI Models in Action” (this is a guided PT sim where you trace a web request through layers) [78] .

- **Coursera “Computer Communications” Week 1** (Princeton via Coursera, can audit) – This offers another explanation of layering and introduces Internet design principles. A different perspective can reinforce learning.

- *Hands-On Labs/Projects:*

- **Lab 2.1: Inspecting Packets in Wireshark** – Install **Wireshark** (free packet analyzer). Use Packet Tracer’s built-in Sniffer or your own PC’s ping. In PT: connect a PC to a PT Cloud (internet) and generate traffic, capture it. Alternatively, on your actual computer, ping a site and capture in Wireshark. Inspect an ICMP packet: identify the Ethernet frame header, IP header, and ICMP data. **Expected Outcome:** You can see the different protocol headers layered (Ethernet contains IP which contains ICMP). Take a screenshot labeling the layers.
- **Lab 2.2: Basic Switch Configuration** – In Packet Tracer, place a 2960 switch and a PC. On the switch CLI, practice commands: set hostname (`hostname Week2Switch`), set a **banner** message (`banner motd "Authorized Access Only"`), configure an IP on the switch’s VLAN1 interface (e.g. 192.168.1.10/24) so you could manage it, and set up a login password on

the console. Also practice the `show interface status` and `show running-config`.
Expected Outcome: You become familiar with user EXEC vs config mode, and you have a switch with basic settings. Save the PT file for reuse.

- **Lab 2.3: Media Demonstration** – If you have different cable types in Packet Tracer (copper straight-through vs crossover vs fiber), set up a simple test: e.g. connect two switches with the wrong cable type and observe link down, then correct it. This will reinforce cable differences (Copper crossover for switch-switch if no auto-MDIX, fiber needs fiber ports, etc.).

- *Quizzes/Assessments:*

- **Week 2 Quiz (30 questions)** – Covering OSI vs TCP/IP layers, protocol examples, TCP vs UDP differences, and basic Cisco CLI commands. Sources: Try creating a custom quiz in a tool like Quizlet, or use exam prep books' chapter questions. Ensure you can answer: "Which OSI layer does XYZ occur?", "What's the advantage of TCP over UDP and vice versa?", "Which cable for connecting two switches?" etc.
- **NetAcad Module 3 Quiz** if using NetAcad.
- Continue adding to Anki: e.g. flashcards for "TCP vs UDP – which is connection-oriented?", "Default port for HTTP?", "Command to set switch hostname?", etc. Aim for ~15 new flashcards this week.

Time Allocation (~13 hours):
- Videos: ~3 hours (models, protocols, TCP/UDP)
- Reading: ~3 hours (Cert Guide chapters, articles)
- Labs/Practice: ~4 hours (Wireshark hands-on, switch CLI config, cable experiments)
- Quizzes/Flashcards/Review: ~2–3 hours (includes Anki and discussing tricky quiz answers in forums or study group)

Milestones & Checkpoints:
- **Milestone 1:** Write a short explanation (half-page) comparing **TCP vs UDP** in your own words. Include an example application for each (e.g. "TCP for HTTP web pages because…, UDP for live video streaming because…"). This checks your understanding of reliability vs speed trade-offs.
- **Milestone 2:** Complete the Wireshark lab and save a screenshot of a dissected packet. Label the Ethernet, IP, and TCP/UDP headers in your screenshot as a mini-report.
- **Milestone 3:** Configure a Packet Tracer switch with a hostname and IP, and **successfully ping it from a connected PC** (means your config was correct). Save this PT file as "Week2_SwitchConfig.pt".
- Achieve at least **25/30** on the Week 2 Quiz. For any missed questions, write down an explanation after researching the answer – this will turn mistakes into learning.
- **Checkpoint:** You should now be comfortable with fundamental terminology and able to navigate the CLI basics. If terms like "encapsulation", "segment vs packet", or any layer functions are still confusing, revisit the OSI chart or ask for clarification on forums (Cisco Learning Network community is helpful).

Motivation: Two weeks in, great work! At this point you've laid the groundwork that many find abstract – but these concepts pay off later when we configure protocols. Keep remembering **why you're doing this**: each protocol or model piece you master is a tool in your belt for real-world troubleshooting. If you find yourself struggling, don't hesitate to revisit resources or try a different medium (video vs text). The next couple of weeks we'll dive into IP addressing – arguably the heart of networking. Stay curious and keep up the momentum!

Week 3: IP Addressing & Subnetting (Fundamentals Part II)

Objectives (Week 3):
- Understand **IPv4 addressing** thoroughly: the format of an IPv4 address, binary representation, network vs host portions, and the role of the subnet mask.
- Learn how to **subnet** IPv4 networks: given requirements (like X subnets or Y hosts), be able to calculate appropriate subnet masks, network IDs, broadcast addresses, etc. This is a crucial skill for the exam and real life.
- Practice configuring IP addresses on devices (routers, PCs) and verify connectivity within and across subnets.
- Get introduced to **private IP vs public IP** and the need for NAT (we will configure NAT later, but concept starts here) [79] .
- Briefly overview **IPv6 basics**: understand the IPv6 address format, why IPv6 was introduced, and the different address types (global, link-local, unique local, multicast) [12] [13] . We will do more IPv6 in Week 4, but start familiarizing now.

Resources:
- *Videos/Tutorials:*
- **"IPv4 Addressing Basics"** (Cisco Networking Academy YouTube, ~15 min) – Explains how IP addresses and subnet masks work, with examples.
- **NetworkChuck "Subnetting Masterclass"** (YouTube, ~30 min) – Chuck demonstrates a quick method to subnet, using his energetic style. He covers binary math in an accessible way.
- **Jeremy's IT Lab Day 7 & 8 – IPv4 Addressing Part 1 & 2** (YouTube, ~40 min total) – In-depth subnetting lectures [80] [81] , including practice problems (Jeremy breaks down the process step-by-step). Highly recommended – follow along and do the exercises he presents.
- **"IPv6 Basics"** by Sunny Classroom (YouTube, 20 min) – Simple explanation of IPv6 address notation, types, and how it differs from IPv4. A good intro before diving deeper next week.

- *Books/Chapters:*
- **CCNA Cert Guide (Vol. 1)** – Read Chapter 11: *IP Addressing* (covers IPv4 addressing and intro to subnetting). Work through the examples in the chapter by hand. Then read Chapter 12: *Subnetting* and **do the practice problems** provided. Odom's books have practice questions at chapter ends – ensure you attempt those.
- **"31 Days Before Your CCNA"** (if available) – Day 5 and 6 cover IPv4 and subnetting in a concise way, with practice quizzes. This can be a quick refresher once you learn from Odom.
- **Computer Networking (Kurose/Ross)** – Section 4.3 covers IP addressing and CIDR. It offers a conceptual view (skip heavy details on routing algorithms for now).

- *(Reference)* **Subnetting Cheat Sheet** – find a reliable cheat sheet (like one on IPCisco or Cisco's site) [82] that lists common subnet sizes (/24, /25, /26, ... /30) with their block size, number of hosts, etc. Keep this for reference initially, but aim to memorize key subnet values over time.

- *Research Papers/Articles:*

- **RFC 1918 – Address Allocation for Private Internets** – skim this to see the official private IP ranges (10.0.0.0/8, 172.16/12, 192.168/16) and understand why/how they're reserved.
- **"Subnetting – Why and How"** (Cisco Blog or PacketLife article) – an article explaining real-world use of subnetting (segmentation, reduced broadcast domains).
- **Cisco Press Article: "IPv6 Address Types"** – outlines global vs link-local vs unique local, etc., in a straightforward manner. This complements the brief IPv6 intro from videos.

- *(Optional, deep dive)* **“IPv4 Address Exhaustion and NAT”** – any networking journal article discussing how IPv4 exhaustion led to NAT and IPv6 (if curious about the bigger picture).

- *Online Courses:*

- **Cisco NetAcad – ITN v7 Modules 8 & 9**: These modules cover IP addressing and subnetting with interactive examples. Do the lab exercises like “Subnetting scenario” if provided. NetAcad also has a *Subnetting Game* in some courses – use it to practice in a fun way.

- **Udemy Free Subnetting Course** (if any exist, or simply find a free worksheet online) – Some instructors have free sections or practice sets for subnetting. Timed subnetting quizzes help build speed (e.g., “subnetting in your head” challenges).

- *Hands-On Labs/Projects:*

- **Lab 3.1: Subnetting Practice (Paper or Tool)** – Not a typical lab, but spend time *manually calculating* subnets. For example, take a Class C network 192.168.10.0/24 and practice making: (a) 2 subnets (each /25), (b) 4 subnets (/26), (c) 8 subnets (/27). Write down the subnet ID, broadcast, and valid host range for each. Do similar for a /16. Use a whiteboard or spreadsheet if needed. Check answers with a subnet calculator to verify.
- **Lab 3.2: Configure Subnets in Packet Tracer** – Build a small network with **3 subnets**: e.g., one for Branch1 PCs, one for Branch2 PCs, and one for the WAN link between two routers. For instance: Router A (Branch1) with PC network 192.168.1.0/24, Router B (Branch2) with PC network 192.168.2.0/24, and a /30 for the link between routers. Configure IPs on two routers’ interfaces and on a PC in each subnet. Use static routes (we haven’t formally covered yet, but you can guess or look up how to add a static route) to ensure the two PCs can ping each other through the routers. **Expected Outcome:** Both PCs, in different IP networks, communicate via the routers (verifying your addressing and basic routing config). This is a preview of Week 4’s routing topics but reinforces addressing.

- **Lab 3.3: IPv6 Addressing Basics** – In Packet Tracer, enable IPv6 on a router and a PC: assign a global IPv6 address (e.g., 2001:DB8:1::1/64 on router, 2001:DB8:1::2/64 on PC) and a link-local (should auto-generate). Ping the link-local and global addresses to test connectivity. If unfamiliar with IPv6 config, use a guide. **Expected Outcome:** You can configure and verify IPv6 addressing on Cisco IOS and understand the abbreviations. Document one example of an IPv6 address you used and identify its parts (network prefix, interface ID).

- *Quizzes/Assessments:*

- **Subnetting Speed Quiz:** time yourself to find answers to 5 subnetting questions (e.g., “How many hosts in a /27?”, “What is the subnet mask for 4 subnets of /24?”). Resources like subnettingpractice.com or random question generators help. Aim to get each within 1-2 minutes without referring to notes.
- **Boson ExSim (if available) Subnetting section** – Boson practice exams have great subnetting questions. If you have access, try a subset. If not, use free question dumps carefully on ExamTopics – focus on understanding, not memorizing answers.
- **Chapter-end questions from Odom** – do all at end of IP addressing chapters.
- Continue adding flashcards: e.g., “Subnet mask /26 = ? 255.255.255.192, hosts?”, “Private IP ranges?”, “IPv6 link-local prefix?”. Daily review previous cards – by now ~30+ cards in deck.

Time Allocation (~14 hours):
- Concept videos: ~2 hours (more time should be on practice than videos now)

- Reading & Note-taking: ~3 hours (addressing chapters, articles)
- Subnetting practice (paper/calculations): ~3 hours (spread out in sessions)
- Packet Tracer labs: ~4 hours (multi-subnet network, IPv6 config)
- Quizzes & flashcards: ~2 hours (including timed practice)

Milestones & Checkpoints:
- **Milestone 1:** Be able to **subnet a network in under 10 minutes** for a given scenario. For example, "Design an IP scheme for a company with 3 departments (50 hosts, 30 hosts, 20 hosts). What subnets do you use out of 192.168.10.0/24?" – Write out your solution and rationale.
- **Milestone 2:** Complete Lab 3.2 (2-router, 2-PC network) and demonstrate a successful ping from a PC on Router A's network to a PC on Router B's network. This shows you can correctly assign IPs and even set a basic static route. Save this lab as "Week3_RoutingIntro.pt".
- **Milestone 3:** List the three private IPv4 ranges from memory and explain in a few sentences *why* private addresses need NAT to reach the Internet. Similarly, list at least two types of IPv6 addresses (e.g., "Link-local starts with FE80, used only on local link").
- **Checkpoint:** By end of Week 3, *subnetting should feel more comfortable.* If you still struggle, schedule extra practice – it's that important. Consider using a **subnetting app or game** daily for speed. Also check that you haven't neglected earlier topics: try explaining to yourself how OSI layers relate now that you've added IP (Layer3) knowledge.

Motivation: Subnetting is often a hurdle for beginners – if you've cracked it this week, give yourself a pat on the back! If not, don't panic; it *will* click with continued practice. Many find it helpful to teach someone else (or an imaginary student) the process – this solidifies your mastery. You're now halfway through the fundamentals phase. Keep up the disciplined study habits. Next week we'll wrap up Network Fundamentals with more on IPv6, wireless, and some network services.

Week 4: Wrapping up Fundamentals (IPv6, Wireless, Visualization, Review)

Objectives (Week 4):
- Solidify understanding of **IPv6**: cover address types in more detail (global unicast, unique local, link-local, multicast, anycast) and IPv6 configuration on Cisco devices (SLAAC, DHCPv6 concepts).
- Learn basic **network troubleshooting tools**: `ping`, `traceroute`, and OS commands to verify IP configuration (`ipconfig`/`ifconfig` on host OSes) [83]. By CCNA blueprint, you should know how to verify IP parameters on Windows, Mac, Linux.
- Explore **wireless fundamentals**: non-overlapping Wi-Fi channels (2.4GHz vs 5GHz), what an SSID is, basics of Wi-Fi security (WPA2). This ties into Network Fundamentals (1.11 wireless principles) and Security Fundamentals (5.9 wireless security protocols) [84].
- Introduction to **network virtualization**: concepts of VLAN (virtual LAN) vs VRF vs VPN (just definitions; we will *configure* VLANs in Month 2, but here understand that virtualization allows multiple networks on same physical infrastructure). Also understand what a **server virtualization** and **container** means in networking contexts [85] (to meet 1.12 blueprint).
- Conduct a **Month 1 review**: revisit all main topics (devices, OSI, TCP/UDP, addressing). Identify any weak areas before moving to Month 2.

Resources:
- *Videos/Tutorials:*
- **"IPv6 Address Types"** (KEITH Barker YouTube, ~20 min) – Keith (or similar instructor) explaining global vs local vs link-local addresses, multicast, and how IPv6 addresses auto-configure.
- **Jeremy's IT Lab Day 31-33 – IPv6 Parts 1-3** (YouTube, ~30 min each) – These cover IPv6 addressing and configuration in detail. Perhaps focus on Day 31 (IPv6 basics) and Day 32 (configuring IPv6) for now, and we can revisit Day 33 later for advanced IPv6 routing concepts.

- **“Wireless Networking Basics”** (Cisco or CompTIA Network+ channel, ~15 min) – Introduction to Wi-Fi standards (802.11), frequencies, channels, and security basics.
- **“Intro to VLANs”** (NetworkChuck, 10 min) – Though we’ll do VLANs next month, watch this short video to conceptualize network segmentation (it reinforces the idea of virtualization at Layer2, part of blueprint 1.12).
- *(Optional)* **“Basic Troubleshooting Tools”** (CBT Nuggets or Professor Messer, 10 min) – A quick overview of using ping, traceroute, etc., on different OSes.

- *Books/Chapters:*
- **CCNA Cert Guide (Vol. 1)** – Read Chapter 13: *IPv6 Addressing & Subnetting*. Focus on the sections about IPv6 address types and the configuration examples (don’t get bogged down in IPv6 subnetting – just know it conceptually, since CCNA may have a few IPv6 questions but not heavy calculation).
- **Cert Guide Chapter 5: Network Protocols** (if not already covered) – Contains a section on ICMP (ping, traceroute) and basic DHCP/ARP concepts. This ties up some loose ends in fundamentals (knowing ARP as a link-layer address resolution, for example).
- **CWNA (Certified Wireless Network Administrator) Study Guide** (if accessible) – skim the intro chapter on WLAN fundamentals to understand SSID, channels, and basic wireless security. Alternatively, any **Cisco Press Wireless Fundamentals** chapter if available.

- **Virtualization/Cloud Basics:** A short chapter or whitepaper on virtualization (e.g., “Intro to Virtualization” by VMware or Cisco’s Network Virtualization whitepaper) – focus on the idea of running multiple logical networks on one physical set of devices (this concept underlies VLANs, VRFs, and SDN).

- *Research Papers/Articles:*

- **Cisco Blog: “IPv6 – The Next Generation Internet”** – an article by Cisco explaining why IPv6 is important, with some real-world adoption info.
- **“The TCP/IP vs OSI Debate”** – historical perspective article on why both models exist. (Good read to wrap up your understanding of models.)
- **Cisco Whitepaper: “Networking in Virtualized Environments”** – describes challenges and solutions when multiple VMs share a host (introduces virtual switches, etc.). Just read the overview to fulfill blueprint 1.12 context.

- **OSI Model Quiz/Chart** – one more glance at a reference (StationX OSI cheat sheet [86] or similar) to ensure you can mentally map all layers after learning these services (e.g., know that ping uses ICMP at Layer3, traceroute also uses Layer3, etc.).

- *Online Courses:*

- **Cisco NetAcad – Module 10 (IPv6 Addressing)**: Go through this module, which includes activities on configuring IPv6 addresses and maybe an IPv6 Packet Tracer exercise.
- **Cisco NetAcad – Module 17 (Network Troubleshooting)**: This might be in the later part of the course; if accessible, check out the portion on using ping and traceroute effectively.

- **Labs from previous weeks**: Consider redoing any NetAcad Packet Tracer labs now without looking at instructions, as a self-test.

- *Hands-On Labs/Projects:*

- **Lab 4.1: IPv6 Neighbor Discovery** – Extend Lab 3.3 (the IPv6 lab). Configure two routers connected via IPv6. Enable OSPFv3 or simply static routes for IPv6 to see end-to-end connectivity. Also, test the **SLAAC** feature: on a router interface, enable it to advertise a prefix (turn on IPv6 unicast-routing and use `ipv6 address prefix/64 eui-64` on interface, or SLAAC configs). Configure a PC to get an IPv6 address automatically. **Expected Outcome:** The PC autoconfigures a global IPv6 address (stateless) and can reach the router. Check the PC's IPv6 config to see link-local and autoconfigured addresses.
- **Lab 4.2: Wireless Router in Packet Tracer** – PT has generic wireless routers. Set up a PT home wireless router, give it an SSID "Week4WiFi" with WPA2 password, and add a PC with a PT wireless NIC to connect to it. See if you can ping between wireless PC and a wired PC on that router. **Expected Outcome:** Understand how a wireless client associates via SSID/security to an AP. (This lab is limited but gives a conceptual demo. Real gear would be needed for full effect, but PT can simulate a bit.)
- **Lab 4.3: Basic Troubleshooting Scenarios** – Deliberately break things in a small PT network and practice troubleshooting: e.g., take a simple two-router network and misconfigure IP on one side, or use wrong default gateway on a PC, then use `ping` and `traceroute` from the devices to identify the issue. Document one scenario: describe the symptoms (e.g., PC1 can't reach PC2), your troubleshooting steps (ping X, got no reply, etc.), the identified problem, and the fix.

- *(Project)* **Fundamentals Summary Mind-Map:** As a wrap-up for Month 1, create a visual mind-map or diagram that connects the concepts learned: Show how OSI layers relate to specific protocols (HTTP at Layer7, TCP at Layer4, IP at Layer3, Ethernet at Layer2), list device types and where they operate, illustrate an IPv4 vs IPv6 address example, and indicate how subnetting breaks a network. Making this map will reinforce the holistic view.

- *Quizzes/Assessments:*

- **End-of-Month Fundamentals Exam:** Take a comprehensive practice test on all topics covered in Month 1 (maybe 50 questions). You can use a mix of resources: some questions from ExamTopics (filter by fundamentals), some from Odom's end-of-part quizzes, or a free online CCNA fundamentals test. Treat it like a real exam: timed 60 minutes for 50 questions.
- **Boson ExSim lite**: If you have Boson, perhaps attempt a subset of one exam focusing on early-domain questions.
- **Skill drill**: Perform a "Layer-by-Layer" drill – for a given scenario (like loading a webpage), verbally walk through each OSI layer and what happens. This isn't a formal quiz but a cognitive exercise to test integrated understanding. Possibly do this with a friend or mentor if available, or record yourself.

Time Allocation (~12 hours):
- Videos: ~2 hours (IPv6 and wireless intros)
- Reading: ~2 hours (IPv6 chapter, wireless section, virtualization article)
- Labs: ~5 hours (IPv6 configs, wireless PT, troubleshooting practice)
- Review & Quizzes: ~3 hours (including the 50-question test and analysis of answers, plus assembling the mind-map project)

Milestones & Checkpoints:
- **Milestone 1:** Configure IPv6 on two routers and two PCs (as in Lab 4.1) so that all devices can ping each other's IPv6 global addresses. This confirms understanding of IPv6 addressing and basic routing. Save lab "Week4_IPv6.pt".
- **Milestone 2:** Write a short explanation of a real-world scenario using each **wireless security protocol**

(e.g., “WPA2 is currently common for home Wi-Fi, WPA3 is newer and more secure, WEP is obsolete”). Also list 3 non-overlapping channels in 2.4GHz (1, 6, 11) to demonstrate wireless basics knowledge.
- **Milestone 3:** Complete the Month 1 practice exam (50 Qs) with a score of ~80% or higher. Review each wrong answer and write down why the correct answer is correct. If score < 80%, identify weak areas and plan a revision in Week 5 (we can allocate some review time then).
- **Checkpoint: Fundamentals phase complete!** You should now be confident in network foundational concepts. Verify that you have: a solid grasp of IP addressing and can do subnetting relatively quickly; familiarity with the CLI; understanding of how different network components function and interact. Any lingering confusion here should be addressed before moving on, as Months 2–4 will build on this foundation. Don’t hesitate to use community forums or study groups to clarify doubts.

Motivation: Month 1 down – awesome job. Many newcomers falter at the abstract concepts stage, but you’ve persevered. Now you have a base to build on. Take a moment to reflect on how much you’ve learned in just four weeks. Networking might still feel vast (it is), but piece by piece, you are conquering it. **Stay curious and stay disciplined.** Next month, we’ll start configuring networks in earnest (VLANs, routing, etc.), which is where the fun really begins because you’ll make things *work*! Enjoy a well-deserved rest day before Month 2, and maybe reward yourself (you’ve earned it!).

Month 2: Network Access and Switching Essentials (Fundamentals Part III + Intro to Network Access)

Focus: Month 2 transitions from pure theory into more hands-on **switching and network access** topics. We’ll cover the CCNA Network Access domain (VLANs, STP, EtherChannel, wireless LANs in more depth) and finish any remaining fundamentals (like ARP, DHCP basics) as they tie in. By the end of Month 2, you’ll have configured VLANs, understood how switches prevent loops with STP, and set up a basic wireless LAN. We’ll also continue practicing subnetting and introduce more troubleshooting and design thinking. **Domains covered:** Network Access (CCNA domain 2.0) in-depth, plus relevant IP Services basics (DHCP, ARP) and revisit Network Fundamentals concepts in practice.

Week 5: VLANs and Inter-VLAN Routing

Objectives (Week 5):
- Understand **VLAN concepts**: what VLANs are, how they provide network segmentation at Layer 2, and default VLAN behavior [87] .
- Learn to **configure VLANs** on Cisco switches: create VLANs, assign switch ports to VLANs (access ports) [15] , understand the concept of the **management VLAN** and native VLAN.
- Implement **Inter-VLAN routing**: since different VLANs are different subnets, you need a router or Layer 3 switch to route between them. We’ll configure **Router-on-a-Stick** (a router with subinterfaces for each VLAN) to enable devices in different VLANs to communicate.
- Practice **troubleshooting VLAN issues**: e.g., mismatched VLANs, incorrect IP addressing for VLANs.
- Reinforce subnetting with a real config: design IP subnets for each VLAN in a network and apply them.

Resources:
- *Videos/Tutorials:*
- **“VLANs Explained”** by Kevin Wallace (YouTube, 20 min) – Great conceptual intro to VLANs, why we use them, with simple diagrams.
- **Jeremy’s IT Lab Day 12 – VLANs** (YouTube, ~30 min) – Goes into normal-range VLAN config, access ports, verifying VLANs on a switch, etc.
- **NetworkChuck “Router on a Stick”** (YouTube, 15 min) – Demonstrates inter-VLAN routing using a router with subinterfaces, with a bit of fun flair. This helps visualize how one router interface can handle

multiple VLANs via trunk.
- **CBT Nuggets "Inter-VLAN Routing"** (if you have access, ~15 min) – shows configuration on a Layer 3 switch as well as router-on-a-stick. If no CBT, look for another free video on inter-VLAN routing (e.g., David Bombal has some).

- *Books/Chapters:*
- **CCNA Cert Guide (Vol. 1)** – Read Chapter 10: *LAN Switching Fundamentals* and Chapter 11 (if present in Vol1) or relevant sections on VLANs and trunking. Pay attention to commands like `switchport mode access`, `switchport access vlan X`, `vlan database` vs VLAN config mode (depending on IOS). Also read the part on **802.1Q trunking** – what it is and how the native VLAN works [16] .
- **Official Cert Guide (Vol. 2)** – If Vol.2 covers Inter-VLAN routing, read that chapter (likely early in Vol2). It will explain router-on-a-stick configuration and multilayer switching.
- **"CCNA 200-301 Network Access" (Odom's condensed notes)** – If available, Cisco Press often has an exam review guide summarizing VLAN and STP topics. Use it to review key points after learning.

- Lab manual: **"31 Days Before CCNA"** – see if there's a day on VLANs or trunking and do the exercises.

- *Research Papers/Articles:*

- **Cisco Document: "Configuring VLANs"** – official Cisco docs on VLAN config (on Catalyst switches). Skim for any best practices (like naming VLANs, using VLAN 1 or not, etc.).
- **"The Death of VLAN 1"** (blog) – an article explaining why you should not use VLAN 1 for management (common security advice). This adds real-world flavor to your VLAN knowledge.
- **Cisco Support Forum thread on Router-on-a-Stick** – read a Q&A or troubleshooting case to see common mistakes (e.g., forgetting to set the router port as trunk or mismatched native VLAN).

- *(Design)* **"LAN Segmentation and VLANs"** – chapter from an older Cisco design guide or whitepaper explaining how VLANs are used in network design. Focus on the rationale (security, reduce broadcasts, etc.).

- *Online Courses:*

- **Cisco NetAcad – Switching, Routing & Wireless Essentials (SRWE) v7**: If you finished ITN, the second course SRWE covers VLANs early on. Complete Chapter 2: VLANs, and Chapter 3: Inter-VLAN Routing. There will be Packet Tracer labs for both (do them!).
- **Labs from Packet Tracer Tutorials** – Cisco PT has some built-in sample labs (check "Open Sample" in PT). Look for any labeled VLAN or trunking to practice.

- **Udemy (optional)** – If you find a cheap CCNA lab course, you can do a VLAN lab with them; but likely your own practice is enough.

- *Hands-On Labs/Projects:*

- **Lab 5.1: VLAN Configuration and Ping Test** – In Packet Tracer, set up one switch with 3 PCs on it. Create 2 VLANs (say VLAN10 and VLAN20). Put 2 PCs on VLAN10, and 1 PC on VLAN20. Assign IP addresses such that PCs in different VLANs are on different subnets (e.g., VLAN10 uses 192.168.10.0/24, VLAN20 uses 192.168.20.0/24). Initially, do *not* configure any router. Verify that two PCs in the same VLAN can ping each other (should work), but PCs in different VLANs cannot (expected, since no inter-VLAN routing yet). This shows VLAN segmentation.

- **Lab 5.2: Router-on-a-Stick** – Extend Lab 5.1 by adding a Router (2911 or similar in PT) and connecting the switch to the router with one link. Configure that switch port as a **trunk** (`switchport mode trunk`) and on the router configure subinterfaces: e.g. `Gig0/0.10` for VLAN10, `Gig0/0.20` for VLAN20, assign 192.168.10.1 and 192.168.20.1 respectively. Don't forget `encapsulation dot1Q 10` etc. Now set each PC's default gateway to the router's subinterface IP (PCs in VLAN10 use 192.168.10.1). **Expected Outcome:** PCs in different VLANs can now ping each other through the router. Also test pinging the router gateways. Save this lab as "Week5_VLAN_RouterOnStick.pt".
- **Lab 5.3: Trunking and Native VLAN** – Add a second switch to Lab 5.2, connected via a trunk link to the first switch. Put one PC on the second switch on VLAN10. Ensure trunk is up (use `show interfaces trunk`). The PC on switch2 VLAN10 should communicate with PCs on switch1 VLAN10. Experiment by changing native VLAN on one side and see the effect (noticing errors or ping issues if mismatched). Then set them correctly. **Expected Outcome:** Understanding of how trunks carry multiple VLANs and the importance of matching native VLANs.

- *(Mini-Project)* **VLAN Design Document:** Imagine a small office network for a company with 3 departments (e.g., Sales, Engineering, Guest WiFi). Sketch a simple network diagram showing 3 VLANs, how they connect to a router or L3 switch for inter-VLAN routing, and propose an IP range for each. Write a paragraph justifying the VLAN segmentation (e.g., "to isolate guest traffic from internal", etc.). This is a design exercise to apply VLAN knowledge conceptually.

- *Quizzes/Assessments:*

- **VLAN/Trunking Quiz:** ~15 questions focused on VLAN concepts. E.g., "What command assigns a port to VLAN 10?", "Which VLAN ID range is normal vs extended?", "What is the purpose of the native VLAN?", "True/False: Devices in different VLANs can communicate without a router." Use CCNA exam prep question banks or the NetAcad chapter quiz.
- **Inter-VLAN routing quiz:** ~10 questions on router-on-a-stick config (e.g., identify missing config in a scenario, or understand subinterface numbering).
- **Review past topics:** include 5 mixed questions from Month 1 topics (to keep memory fresh).
- Flashcards: add key VLAN-related commands and concepts (e.g., "Default VLAN = ? (VLAN1)", "802.1Q tag adds how many bytes? (4 bytes)", "Router-on-a-stick requires what encapsulation command?", etc.).

Time Allocation (~13 hours):
- Videos: ~2 hours (VLAN + inter-VLAN demos)
- Reading: ~2 hours (Cert Guide + articles)
- Labs/Practical: ~6 hours (it will take time to configure, test, troubleshoot VLAN labs, especially trunking with multiple switches)
- Quizzes & flashcards: ~2 hours
- Note consolidation: ~1 hour (documenting lab results, updating your notes with configurations done and lessons learned)

Milestones & Checkpoints:
- **Milestone 1:** Successfully implement a router-on-a-stick with at least 2 VLANs and verify connectivity **between** VLANs via the router. Confirm by screenshotting ping tests from a PC in VLAN10 to a PC in VLAN20, along with a `show ip interface brief` on the router showing subinterfaces up.
- **Milestone 2:** Describe in your notes the difference between an **Access Port** and a **Trunk Port**. List the commands to configure each. Also note the typical native VLAN (default 1) and how to change it.

- **Milestone 3:** Score 80%+ on the VLAN/Inter-VLAN quizzes. If any VLAN concept is wrong (for example, confusion about extended VLAN range or how trunk tagging works), revisit that portion in Odom or videos until clear.
- **Checkpoint:** You've now done substantial switch configuration. Ensure you can confidently navigate `show vlan`, `show interfaces trunk`, and understand what it means. If possible, discuss with a peer or in a forum one of your labs (explaining what you did helps cement knowledge). Heading into Week 6, we'll tackle Spanning Tree and EtherChannel, which build on the VLAN/trunk knowledge. Make sure trunking is solid in your mind (we'll see why STP is needed when redundancy is introduced).

Motivation: Setting up VLANs is your first real network *engineering* task – you segmented a network and made them talk. This is exactly what network engineers do in enterprises. Reflect on how far you've come from "what is a network" to actually configuring multi-VLAN networks! The first time is always the hardest; it gets easier. If things didn't work initially, that's normal – troubleshooting and figuring out *why* (maybe a missing `encapsulation` command or mis-assigned port) is where real learning happens. Embrace those moments. Keep this momentum into Week 6.

Week 6: Spanning Tree and EtherChannel (Switch Resiliency)

Objectives (Week 6):
- Understand the **Spanning Tree Protocol (STP)**: why it exists (prevent switching loops), how it elects a root bridge and manages port states (forwarding/blocking) [19] [20]. Learn the basics of Rapid PVST+ (the Cisco default spanning tree mode) and terms like *Root Port, Designated Port, Blocking/Alternate Port* [88].
- Configure STP settings on switches: not in-depth (CCNA is limited here), but know how to identify the root bridge (`show spanning-tree` output) and adjust priorities to influence root election, if required.
- Learn about **EtherChannel (Link Aggregation)**: purpose (increase bandwidth and provide redundancy by bundling links) [18]. Understand the protocols LACP (open standard) vs PAgP (Cisco proprietary) for negotiating EtherChannels.
- Configure a simple **EtherChannel** between two switches in Packet Tracer using LACP (since PT supports it). Verify with `show etherchannel summary`.
- Continue **wireless and security fundamentals**: If not covered yet, ensure understanding of how enterprise wireless differs (AP & WLC architectures, which we'll touch in Week 7) and how spanning tree and EtherChannel might interplay with Wi-Fi (mostly separate topics but complete the network access domain fully).
- Integrate knowledge with a larger lab: by now, you know VLANs, routing, STP, EtherChannel – attempt a lab combining these (see Hands-On).

Resources:
- *Videos/Tutorials:*
- **"Spanning Tree Protocol Basics"** by Keith Barker (YouTube, 30 min) – Keith often uses animations to show how STP elects root and blocks certain ports to break loops. This is valuable to visualize the process.
- **Jeremy's IT Lab Day 13 – Spanning Tree** (YouTube, ~20 min) – Focuses on the need for STP and basics of port roles/states. Jeremy keeps CCNA STP coverage straightforward.
- **NetworkChuck "Spanning Tree in 5 Minutes"** (YouTube, 5 min) – a high-level quick recap of STP (for a bit of fun revision).
- **"EtherChannel Explained"** by David Bombal (YouTube, 15 min) – Shows EtherChannel config and verification, plus common mistakes (like ports not matching settings).

- **CBT Nuggets “EtherChannel”** (if access, 10 min) – Another demonstration, perhaps using real equipment. If not, the free Bombal video suffices.

- *Books/Chapters:*
- **CCNA Cert Guide (Vol. 1 or 2)** – Find the section on Spanning Tree Protocol (likely in Vol.2 under LAN switching). Read the parts about *STP operations*, *RSTP improvements*, and the CCNA-level detail of PVST+ (per-VLAN STP). Note: memorize STP port states (Blocking, Listening, Learning, Forwarding, Disabled) and port roles (Root, Designated, Alternate) – Odom’s text will cover these clearly.
- Also read about **Layer 2 EtherChannel** in the Cert Guide. Focus on configuration guidelines (all member ports must have same speed/duplex, be in same VLAN or trunk mode, etc.) and LACP modes (`active/passive`).
- **“Spanning Tree Protocol” (Cisco Press Chapter)** – if you have a CCNA or CCNP Switching book, one chapter on STP will reinforce your understanding. Pay attention to how BPDU (Bridge Protocol Data Units) are used to elect the root and settle port roles.

- **Errata or recent updates:** Check if any CCNA update added topics like *BPDU Guard* or *PortFast* basics (these are mentioned in blueprint: PortFast benefits [89]). If so, read about those features (PortFast allows edge ports to skip STP listening/learning, BPDU Guard disables a PortFast port if unexpected BPDUs seen – important for security).

- *Research Papers/Articles:*

- **IEEE 802.1D spec (overview)** – not suggesting to read the standard, but maybe find a summary article about how the 802.1D Spanning Tree algorithm works. Good for conceptual clarity if interested.
- **Cisco Whitepaper: “Understanding Rapid Spanning Tree (802.1w)”** – an article or doc explaining how RSTP achieves faster convergence than traditional STP. Only read the intro and maybe the part about how port roles differ (alternate/discarding vs blocking).
- **Networking Forum discussions** – find a Q&A on something like “Why did my EtherChannel not form?” or “STP blocking port on redundant link – is it working correctly?” to see real-world application of these concepts.

- **EtherChannel vs STP design** – a blog that explains how EtherChannel can be used to prevent STP from needing to block ports (because from STP’s perspective, an EtherChannel is one logical link). This is more design-oriented but enriches understanding.

- *Online Courses:*

- **Cisco NetAcad – SRWE v7 Module 4: STP** and Module 5: EtherChannel. Go through these chapters, do the Packet Tracer activities such as “4.6.6 Packet Tracer – Investigate STP” (if available) where you can see STP in action, and “5.x.x Packet Tracer – Configure EtherChannel”. These labs align perfectly with our objectives.
- **Lab challenges**: Some online resources have “challenge labs” for CCNA (like showing a network diagram and asking you to configure STP priorities, etc.). If you find one, try it out.

- **Practice exam on L2**: If your study resources have topic-wise exams, take one on “Network Access” at the end of this week to gauge your progress on switching topics.

- *Hands-On Labs/Projects:*

- **Lab 6.1: Spanning Tree Exploration** – Use your Lab 5.3 topology (two switches connected by two links? If not, create a scenario with 2 switches and 2 redundant links between them, plus a couple PCs). By default STP will block one link. Use `show spanning-tree` on each switch to identify the root bridge, root ports, and blocked port. **Task:** Change the bridge priority on one switch to make it the root for VLAN1 deliberately (e.g., `spanning-tree vlan 1 priority 4096`). Observe how STP reconverges and which ports are now forwarding/blocking. Also test PortFast: set one of the PC access ports as PortFast (`spanning-tree portfast` on Cisco). The PC's port should go into forwarding immediately on link up (in PT this might be hard to notice, but conceptually note it). **Expected Outcome:** You can interpret STP status and influence root election. Document which switch became root and which port got blocked and why.
- **Lab 6.2: Configure EtherChannel (LACP)** – Take two switches with 4 connections between them (or add additional links to an existing topology). Before EtherChannel, STP would block all but one. Now configure EtherChannel: e.g. on both switches do `interface range f0/1-2`, `channel-group 1 mode active` (LACP active). Do same for f0/1-2 on the other switch (active or passive mode). This should form an EtherChannel bundling two ports. Verify with `show etherchannel summary`. Ensure you assign the EtherChannel (Port-channel1) as trunk or access appropriately. **Expected Outcome:** The EtherChannel comes up (flags "SU" in summary) and STP now sees it as a single link, preventing loops while both physical links carry traffic. Test by sending pings while bringing down one member link to see traffic continues.
- **Lab 6.3: Integrated Network Challenge** – Design a scenario that uses everything from Month 2: e.g., 3 switches in a triangle (redundant connections), with VLANs on each, trunk links between them, an EtherChannel on one side of the triangle, and a router or multilayer switch for inter-VLAN routing. This is a mini-"capstone" for switching. **Example**: Switch1 (VLAN10,20), Switch2 (VLAN10,20), Switch3 (VLAN10,20); connect S1-S2-S3 in a triangle (introducing STP). Put an EtherChannel between S1 and S2 (2 links bundled). Connect a router to S1 for routing between VLAN10 and 20 (router-on-stick). Now predict STP: which switch becomes root (set priorities if needed), which ports block, etc. Configure everything and test pings between hosts in VLAN10 and VLAN20 across different switches. **Expected Outcome:** A functioning network where any host in VLAN10 can reach any host in VLAN20 (via router), and STP is active but no broadcast storms occur (you can test by temporarily creating a switching loop without STP to see the effect if curious—but be careful in PT, it might not emulate broadcast storms well). This lab will be complex; allocate plenty of time and do it step by step. It's okay if it's challenging – better to struggle in practice than in exam or real life.

- *(Project)* **Research Current Tech:** Spend an hour researching **Software-Defined Access (SD-Access)** or modern campus designs just to see how technologies like **Spine-Leaf architecture** (from blueprint 1.2) [90] relate. Write a short note on how traditional STP-based designs differ from fabric (SDN) designs. This is to connect your newly gained traditional network knowledge with where the industry is heading (tying into Automation domain, but lightly).

- *Quizzes/Assessments:*

- **STP Quiz:** ~15 questions: covering root bridge election (e.g., given priorities and MACs, who becomes root?), port states, PortFast/BDPU Guard concept (maybe 1 question if any), and understanding STP output ("Which port is in blocking state on Switch X given this topology?" type). Use NetAcad quiz or exam bank.
- **EtherChannel Quiz:** ~5 questions on config and theory: LACP vs PAgP, requirements for EtherChannel, etc.
- **Week 6 review Quiz:** ~10 mixed questions revisiting VLANs, trunking, routing. Perhaps a mini-case: "PC A cannot ping PC B in another VLAN – what could be the issue?" to integrate knowledge.

- **Boson/ExamTopics practice:** If you have access to a bank of questions, filter some on spanning-tree and attempt them. STP can be tricky in wording, so good to practice exam-like questions.
- Continue Anki: add STP timers (forward delay, max age), default priority, and EtherChannel modes as flashcards. At this point you likely have ~50-60 flashcards – schedule time every couple days to do your reviews (spaced repetition will make recall faster on exam).

Time Allocation (~14 hours):
- Videos: ~2 hours (STP and EtherChannel)
- Reading/detailed study: ~3 hours (Odom chapters on STP/EtherChannel, plus articles)
- Labs: ~7 hours (STP experiments, EtherChannel config, integrated challenge lab)
- Quizzes/Review: ~2 hours (includes analyzing any complex STP questions you got wrong, as understanding those is key)

Milestones & Checkpoints:
- **Milestone 1:** Identify the STP root bridge in your Lab 6.1 and explain *why* it's root (lowest priority/MAC). List the root port on each non-root switch and which port is blocking. If you can do this, you have a practical grasp of STP operation.
- **Milestone 2:** Successfully create an EtherChannel that remains up (no err-disabled ports). Show output of `show etherchannel summary` and `show spanning-tree` (to confirm STP sees the bundled link). Note how STP now treats the bundle – e.g., one port-channel as root port instead of individual links.
- **Milestone 3:** In the integrated network lab, achieve full connectivity and demonstrate redundancy (e.g., if you have a triangle, temporarily shutdown one link and show traffic still flows). Document any troubleshooting you had to do (for learning reflection).
- **Milestone 4:** Scores: Aim for ~80% on STP/EtherChannel quizzes. STP is often tricky, so if you scored lower, pinpoint the confusion (common ones: how tie-breakers work for root port election – usually lowest path cost, then lowest sender bridge ID, then lowest port ID; or misunderstanding PortFast vs normal ports). Clarify these via additional reading or asking an experienced friend/mentor.
- **Checkpoint:** Network Access domain should now be largely covered. Confirm you have covered: VLANs, trunking, STP (Rapid PVST+ basics), EtherChannel, and also wireless AP basics (if not, we will touch WLC more next week). Also, how do you feel about Network Fundamentals content now? These weeks likely reinforced IP addressing (since you used it in VLANs) and OSI (spanning tree is layer 2, routing at layer 3). If any fundamental concept still feels shaky, flag it for extra review.

Motivation: You've completed 1/3 of the journey! By mastering switching, you have opened the door to building robust local networks. STP might have felt a bit abstract (it's under-the-hood magic ensuring loop-free topology), but it's a classic technology – knowing it sets you apart. If EtherChannel config gave you trouble, that's normal; labbing it repeatedly is the key. Now you have quite a few lab files saved – **this is your personal portfolio of configurations**. Keep them safe; you can revisit them as templates or show them to demonstrate skills. Coming up: Month 3 will tackle **routing (IP Connectivity)** – the logic that glues networks together. That's another exciting area where you'll configure routers to handle traffic across networks. Take a deep breath, maybe a day off, and get ready for routing!

Month 3: Routing & IP Connectivity (Core Routing Protocols and Services)

Focus: Month 3 dives into the **IP Connectivity domain (25%)** – configuring and understanding routing. We will cover static routing and the OSPF routing protocol in detail, as well as first-hop redundancy protocols conceptually. We'll integrate IP Services like DHCP, NAT, and NTP as we set up networks that need those services. By the end of Month 3, you will have built multi-router topologies, configured dynamic routing with OSPF, and implemented common IP services in labs. **Domains covered:** Primarily *IP Connectivity* (CCNA 3.0) and parts of *IP Services* (CCNA 4.0) like DHCP, NTP as needed in labs.

Week 7: Static Routing and Redundant Default Gateways

Objectives (Week 7):
- Learn how routers **forward packets** by default: refresh longest-prefix-match routing logic [25] and administrative distance basics.
- Configure **static routes** on Cisco routers: host routes, network routes, default routes (quad-zero) [26] [91]. Understand when to use static routing (small or stub networks) and its limitations.
- Practice troubleshooting routing issues: e.g., missing static route or wrong next-hop causing no connectivity.
- Introduce **First-Hop Redundancy Protocols (FHRP)** concepts: HSRP/VRRP/GLBP (the exam expects you to know what they are and purpose [30], but not to configure them). Understand that they provide a **virtual gateway IP** so that if one router fails, another takes over – ensuring default gateway availability.
- Implement a simple HSRP or VRRP scenario in Packet Tracer if possible (PT supports basic HSRP configuration on routers). This is to visualize how two routers can share an IP for redundancy.
- Revisit **ARP** and how it works in routing: ensure understanding that when a router forwards to next-hop, it uses ARP to get the MAC. This ties back to fundamentals and helps troubleshoot layer 3 vs layer 2 issues.

Resources:
- *Videos/Tutorials:*
- **Jeremy's IT Lab Day 11 – Routing Fundamentals & Static Routing** (YouTube, ~30 min) [92] [93] – Excellent coverage on how routing tables work and step-by-step static route configuration.
- **NetworkChuck "Subnetting & Routing"** or similar (YouTube, ~10 min) – Some quick video showing how packets get routed between subnets, reinforcing the concept we experienced in labs.
- **Cisco CCNA Gold Labs – Static Routes** (if available on YouTube, e.g., a lab walkthrough by David Bombal or Chris Bryant). Visualizing multiple routers and static routes can help.
- **"FHRPs (HSRP vs VRRP vs GLBP)"** by Kevin Wallace (YouTube, ~15 min) – Explains the difference between these redundancy protocols and basic operation (active/standby, etc.).
- *(Optional)* **"Floating Static Routes"** (Keith Barker, 5 min) – Very short explanation of a static route with higher administrative distance to serve as backup (ties into FHRP concept by achieving similar backup effect at routing level).

- *Books/Chapters:*
- **CCNA Cert Guide (Vol. 2)** – Read the chapter on IP Routing (should cover static routing and intro to dynamic routing). Focus on how to configure static routes (`ip route` command variants). There's likely a section on first-hop redundancy in the IP Services part – read that to know definitions of HSRP/VRRP/GLBP (they might not require configuration, but Odom will describe how HSRP works with virtual MAC, etc.).
- **Cert Guide on IP troubleshooting** – If there's a chapter about troubleshooting routing, glean tips like using `ping` and `traceroute` to find where connectivity stops, and checking routing tables.

- **HSRP Configuration Guide (Cisco)** – Skim for context: just see sample config and how routers form active/standby. Not needed to memorize, but helpful if you attempt the optional lab.

- *Research Papers/Articles:*

- **Cisco: "Introduction to Routing"** – a beginner-friendly article on how routers route. Could be on Cisco Learning Network.
- **RFC 5798 (VRRP)** – not to read fully, but maybe the intro and motivation for VRRP (open standard alternative to Cisco's HSRP).
- **Network Computing: "FHRP Comparison"** – an article or blog comparing HSRP, VRRP, GLBP in terms of what they do. Since GLBP (load balancing gateway) is Cisco-proprietary and interesting, note how it differs.

- **Troubleshooting Static Routes** – A support forum or blog scenario where static routes were misconfigured (e.g., wrong next-hop, missing route on one side, etc.), and how it was diagnosed. This will give insight into common pitfalls (like forgetting a route back causing one-way communication).

- *Online Courses:*

- **Cisco NetAcad – SRWE Module 6: Static Routing** and Module 15 (or ENAUTO content) on FHRP (if any). NetAcad has a lab "Configure Static Routing" – do it. Also, they might have a Packet Tracer for HSRP. If yes, try it.
- **Lab Practice** – Some websites (like Free CCNA Workbook) have static routing labs. Use those descriptions to set up scenarios.

- **Packet Tracer Challenge** – Use PT's Activity Wizard or find some PT activities shared online for static routing challenges (like a troubleshooting scenario where you must add missing routes).

- *Hands-On Labs/Projects:*

- **Lab 7.1: Static Routing Basic** – Create a topology of 3 routers in a chain (R1—R2—R3) with three networks: network A between R1 and R2, network B between R2 and R3, and a loopback or LAN off R1 and R3 each to simulate end networks. Without dynamic routing, configure static routes so that: R1 knows how to reach R3's LAN, R3 knows how to reach R1's LAN, and both use R2 as next hop. Also R2 needs routes to both LANs (or use default routes strategically). **Expected Outcome:** End devices on R1's LAN can ping end devices on R3's LAN. Test by pinging across and possibly traceroute to see the path. Document the routing table of each router (`show ip route` output) to confirm the routes.
- **Lab 7.2: Static Route Failover (Floating Static)** – Modify Lab 7.1 by adding a redundant link: e.g., a direct link between R1 and R3 (so we have two paths between R1 and R3: one via R2, one direct). On R1, set a primary static route to R3's LAN via R2. Then set a *floating static* (higher AD) via the direct link. Do the inverse on R3. Test: when everything up, traffic goes via R2 (check traceroute). Shut down the R1-R2 interface to simulate failure; traffic should reroute via direct R1-R3 link thanks to the floating static. **Expected Outcome:** You see failover in action with static routes (this parallels what dynamic routing or FHRP would do automatically). This solidifies understanding of AD (administrative distance) and backup routes.
- **Lab 7.3: HSRP Configuration** (optional if time and interest) – If Packet Tracer supports HSRP on routers (it does on multilayer switches for sure, routers maybe), set up two routers both connected to a LAN (e.g., PC, Switch, and two routers all in VLAN 10). Configure HSRP on the routers for that VLAN10 network: give them a virtual IP as default gateway for the PC. Make one router active with higher priority. Observe that the PC's default gateway is the virtual IP, but it's being served by Router1. Then shut Router1's interface and see Router2 take over (PC should still ping out, perhaps to a simulated internet cloud or another network). **Expected Outcome:** The PC doesn't lose connectivity when the primary gateway router goes down – HSRP provides redundancy. Use `show standby` on routers to see HSRP status.

- **Lab 7.4: Troubleshoot Static Routes** – Intentionally break something in a static route setup: e.g., omit a route on one of the routers and see how ping fails one direction. Practice diagnosing: use `ping`, then `traceroute`, then check routing tables, then fix route. Document this process as if writing a troubleshooting ticket resolution.

- *(Design Exercise)* **Default Gateway Redundancy Plan:** Write a small memo for a hypothetical network: two edge routers serving a network. Propose which FHRP to use (say VRRP if multi-vendor or HSRP if Cisco-only) and why. Outline the config steps at high level. This isn't execution but demonstrates you understand the problem FHRPs solve and how you'd apply it.

- *Quizzes/Assessments:*

- **Static Routing Quiz:** ~10 questions: covering syntax (`ip route` command format), how to interpret a routing table entry, the effect of AD, and maybe a simple scenario question ("PC can't reach server, which static route is missing?").
- **FHRP Quiz:** ~5 questions: mostly conceptual – "What does HSRP provide?", "Which FHRP is Cisco-proprietary vs open?", "How does a host use HSRP – what IP does it have as gateway?", etc.
- **Subnetting/IP review:** Include a few questions to keep subnetting fresh (never stop practicing!). e.g., "Which of these is a valid /30 network address?" or "You need at least 100 hosts, which mask do you choose?"
- **NetAcad Chapter quiz** for static routing (if using NetAcad).
- Continue Anki: static vs dynamic routing definitions, HSRP default port (maybe not needed, but could note HSRP uses virtual MAC starting with 0000.0C07.ACxx – trivia that might appear), command for floating static route (just adding AD at end), etc.

Time Allocation (~12 hours):
- Videos: ~2 hours (routing fundamentals, FHRP)
- Reading: ~2 hours (Cert guide static route chapter, FHRP sections)
- Labs: ~6 hours (static route labs, including failover scenario and possibly HSRP)
- Quizzes/Flashcards: ~2 hours (analysis of mistakes, reviewing tricky parts like VLSM or static route recursion if any)

Milestones & Checkpoints:
- **Milestone 1:** Configure static routes on a multi-router topology and demonstrate end-to-end connectivity. Provide a screenshot of `show ip route` from each router with explanations of each route entry (e.g., "S 10.1.1.0/24 [1/0] via 10.2.0.2" means a static route to network 10.1.1.0 with AD 1 via next-hop 10.2.0.2). Explaining the routing table cements your understanding.
- **Milestone 2:** Achieve a successful static route failover test (if attempted): demonstrate via traceroute or ping that traffic reroutes when primary path is down. This shows grasp of AD and backup routes.
- **Milestone 3:** Be able to describe how HSRP/VRRP works without notes. For example: "HSRP: two or more routers form a group with a virtual IP; one is active (forwarding) with virtual MAC, another is standby; if active fails, standby takes over virtual IP/MAC so hosts don't notice." If you can say that, you're set for CCNA-level FHRP knowledge.
- **Milestone 4:** Static routing quiz score ~100% (it's a small topic, aim to perfect it), FHRP quiz ~80%. If any confusion remains (like difference between GLBP vs HSRP), clarify now.
- **Checkpoint:** You've laid the groundwork for dynamic routing. Static routes are fine but imagine doing that for 50 routers – not scalable. You should be eagerly anticipating how a protocol like OSPF will automate route distribution – that's next week. Also ensure you haven't lost touch with switching: maybe in labs you combined VLANs with routing (router on stick is static route case). If not, maybe quickly review your inter-VLAN lab to see static routes in action (the router had connected routes for

VLANs; static routes might have been used on switches if L3 switch, etc.). Everything's building up. On to OSPF!

Week 8: OSPF – Single-Area Configuration and Theory

Objectives (Week 8):
- Learn what **OSPF (Open Shortest Path First)** is and why dynamic routing protocols are needed. Understand OSPF's general characteristics: link-state protocol, uses Dijkstra's algorithm, forms adjacencies with neighbors, floods LSAs.
- Know OSPF terminology: *Router ID*, *Area* (focus on single-area OSPF, typically Area 0 only in CCNA scope), *DR/BDR* on multiaccess networks like Ethernet [29] , *metric* (cost, based on bandwidth).
- Configure **single-area OSPFv2** on Cisco routers [28] : using `router ospf <process-id>` and `network` statements, or interface `ip ospf` method. Practice a basic OSPF setup on a multi-router topology and verify adjacency formation (`show ip ospf neighbor`) and routes (`show ip route` showing OSPF routes).
- Handle OSPF attributes: set the Router ID manually (and know auto-selection rules), observe that OSPF chooses a DR/BDR on broadcast networks (maybe simulate with 3 routers in one LAN).
- Basic OSPF troubleshooting: e.g., mismatched subnet masks or areas causing no adjacency.
- Cover OSPF for IPv6 (OSPFv3) conceptually – CCNA may not heavily test it, but know that OSPFv3 exists and is similar but separate process for IPv6. If time, configure one OSPFv3 instance for practice.
- Emphasize that OSPF is a key CCNA topic – possibly multiple exam questions, so spend ample time to master fundamentals.

Resources:
- *Videos/Tutorials:*
- **Jeremy's IT Lab Day 14 & 15 – OSPF (Parts 1 & 2)** (YouTube, ~30 min each) – These cover OSPF basics, configuration, neighbor relationships, etc., in CCNA-focused detail [94] [95] . Jeremy often includes lab demos.
- **Keith Barker "OSPF Basics"** (YouTube, ~20 min) – Great conceptual explanation using whiteboard – covers what LSAs are, basic link-state idea, without diving too deep (CCNA doesn't require LSA types memorization, but concept of link-state flooding is good to know).
- **NetworkChuck "OSPF in 7 Minutes"** – Quick high-level recap or introduction to get the gist (as a supplementary resource to keep it fun).
- **David Bombal Lab on OSPF** (if available on YT, e.g., "CCNA OSPF Lab Packet Tracer") – Following along a lab step-by-step can reinforce config and verification commands.
- *(Optional)* **"OSPF Neighbor States"** – if you want to go beyond, some videos explain the states (Down, Init, 2-Way, Exstart, Exchange, Loading, Full) – but at CCNA, just knowing Full adjacency and maybe 2-Way for DROTHERs is enough. If curious, watch a short explanation.

- *Books/Chapters:*
- **CCNA Cert Guide (Vol. 2)** – Read the OSPF chapter very thoroughly. It likely covers single-area config, OSPF operation concepts, neighbor relationships, and troubleshooting tips. Make sure you understand how OSPF identifies neighbors (by matching area, authentication (if any), subnet, hello/dead timers, etc.). For CCNA, main things: matching subnet mask and area must match for adjacency; router ID selection (highest loopback IP or highest active IP if no manual ID); the concept of DR/BDR on multiaccess networks – only one DR/BDR per network segment to reduce adjacencies.
- Any included labs or examples in the text – do them or simulate them in Packet Tracer as you read.
- **"OSPF LSA Types Simplified"** (if in text or an appendix) – not required to memorize types, but reading a summary might help you understand how OSPF shares info (Link State

Advertisements). CCNA might have a question like “Which routing protocol floods link-state advertisements?” or “Which routing protocol uses cost as metric?” which you should easily answer by now.

- If you have a *lab manual or guide*, see if there’s an OSPF exercise; doing more than one OSPF lab is useful.

- *Research Papers/Articles:*

- **RFC 2328** – OSPFv2 Specification (again not to read fully, but maybe the intro and rationale). The first paragraph often states it’s a link-state routing protocol using SPF algorithm.
- **“OSPF Neighbor Troubleshooting Checklist”** (Cisco Support) – gives common reasons two OSPF routers won’t form adjacency (e.g., area mismatch, IP mismatch, passive interface, etc.). Keep this as a reference to troubleshoot your labs if needed.
- **PacketLife OSPF Cheat Sheet** – a one-page summary of OSPF, might list LSA types, state machine, etc. Good for quick review or to see the big picture.
- **Cisco Design Guide excerpt** – maybe a section about when to use single-area vs multi-area OSPF (CCNA doesn’t require multi-area config, but understanding that large networks can be segmented into areas is good).

- *(Industry)* **“Why OSPF is widely used”** – a blog or article extolling OSPF’s scalability, fast convergence, etc., compared to, say, RIP (which is outdated). Just to reinforce you’re learning a relevant protocol.

- *Online Courses:*

- **Cisco NetAcad – Enterprise Networking, Security & Automation (ENSA) v7** likely has OSPF in depth. If available, do Module on OSPF (single-area). They will have Packet Tracer labs like “Configure Single-Area OSPFv2” and maybe an OSPF troubleshooting PT. Do these.
- **Boson NetSim (optional)** if you have it or similar simulation with guided labs, try an OSPF lab scenario.

- **GNS3 labs (optional)** – If you want more realism, you could try a GNS3 or CML lab for OSPF, but Packet Tracer suffices for CCNA-level OSPF.

- *Hands-On Labs/Projects:*

- **Lab 8.1: OSPF Basic Configuration** – Use a 3 or 4-router topology (could reuse static routing lab but remove static routes). Configure OSPF on all routers in Area 0. You can use the `network` commands (e.g., `network 10.0.0.0 0.0.0.255 area 0` to cover certain ranges, or identify each interface). Ensure all routers become neighbors (use `show ip ospf neighbor`). Assign a Loopback interface on one router to observe how OSPF advertises it (it should appear as O IA or O route in others if not area 0? Actually in single area it’s just O). **Expected Outcome:** All routers have routes to all networks via OSPF in their routing tables. Test connectivity across the network.
- **Lab 8.2: OSPF Router ID and Neighbor Relationships** – In the above lab, set router IDs manually (`router-id X.X.X.X`) that are easy to identify (e.g., 1.1.1.1 for R1, etc.). Reload OSPF (clear process) so they take effect. Observe neighbor outputs listing these IDs. Then simulate a multiaccess segment: e.g., connect 3 routers to a single switch (or multi-point cloud) to simulate them on the same Ethernet. See in `show ip ospf neighbor` which one is DR, BDR, DROTHER – by default highest router ID becomes DR. Try changing OSPF priority on one router to make it DR. **Expected Outcome:** Understanding of DR/BDR election – only DR and BDR

show full adjacency with all, others (DROTHER) have 2-way with each other but full only with DR/BDR. For CCNA, just know conceptually, but seeing it is nice.

- **Lab 8.3: OSPF Passive Interface and Default Route** – Take one of your routers (like an edge router) and configure a default route (maybe to a fake internet cloud or a stub network) and inject it into OSPF (using `default-information originate`). Make some interface passive (like LAN interfaces that shouldn't form OSPF neighbor). Ensure OSPF still advertises the connected networks but doesn't try to neighbor on passive interfaces. **Expected Outcome:** Your internal routers receive a default route from OSPF (marked as O*E2 usually), and you understand passive-interface usage (security and efficiency to not send hellos on e.g. user LANs).
- **Lab 8.4: OSPFv3 for IPv6 (optional)** – If eager, configure OSPF for IPv6 on a dual-stack network. Even if just between two routers. This uses `ipv6 ospf` commands on interfaces and `router ospf <id> ipv6`. Verify with `show ipv6 ospf`. Not heavily needed for CCNA, but one lab helps reinforce OSPF knowledge and demystifies IPv6 routing.

- *(Project)* **OSPF Study Notes** – Create a one-page "OSPF cheatsheet" in your own words: including OSPF message types (Hello, LSU, LSA concepts), neighbor requirements, OSPF metrics and default reference bandwidth, and common show commands and their meaning. This act of summarizing will prepare you for any exam question on OSPF as you'll have organized the info yourself.

- *Quizzes/Assessments:*

- **OSPF Concepts Quiz:** ~15-20 questions. Cover OSPF basics: e.g., "What algorithm does OSPF use?" (SPF/Dijkstra), "How does OSPF elect DR?" (highest router ID or priority), "Which multicast addresses does OSPF use for updates?" (224.0.0.5, maybe too deep for CCNA, but possibly trivial Q), "What's the default OSPF cost of a 100Mb link?" (1, since reference BW 100 Mb), etc. Mix concept and config questions.
- **OSPF Configuration Quiz:** ~5 questions focusing on interpretation: e.g., given partial `show running-config`, does OSPF appear correctly configured? Or "Which command verifies OSPF adjacencies?" (show ip ospf neighbor vs show ip route ospf).
- **Troubleshoot scenario Q:** maybe a question: "Router A OSPF config has area 0, Router B has area 1 on their connected link – will they form adjacency?" (Answer: No, area mismatch). Include one or two like that.
- **Review of older topics:** a few questions from switching or static routing just to keep them fresh. Perhaps "What does a switch do if it doesn't know destination MAC?" or "Which command on a switch enables you to see if a port is in err-disabled state?" (to recall STP maybe).
- Flashcards: Expand OSPF deck – e.g., "Default OSPF Hello interval on Ethernet? (10s) Dead interval? (40s)", "OSPF AD? (110) vs EIGRP AD (90) vs static (1) – a bit of comparative knowledge helps.", "Neighbors not forming – check area, masks, timers, auth, MTU". Reviewing these regularly will make OSPF second nature.

Time Allocation (~14 hours):
- Videos: ~3 hours (OSPF requires some time to digest)
- Reading: ~3 hours (this is a heavy chapter likely; do it in segments)
- Labs: ~6 hours (multiple OSPF labs as described; OSPF often requires tweaking and wait times for convergence, so be patient)
- Quizzes/Review: ~2 hours (going through multi-choice and verifying against labs/reading for correctness)

Milestones & Checkpoints:
- **Milestone 1:** Configure a multi-router OSPF network and achieve full connectivity without any static

routes. Provide evidence: e.g., ping from one end to the other *and* the routing table from a router showing OSPF-learned routes. If you trust OSPF's routes and they match expectations (correct subnets and next hops), you did it right.
- **Milestone 2:** Demonstrate understanding of OSPF neighbor relationships. For instance, intentionally misconfigure a parameter (like area) to see adjacency fail, then correct it. Or identify in a multiaccess network which router became DR and why. Jot down a brief explanation of OSPF neighbor states and roles in your notes (even if CCNA doesn't test state names deeply, the process of explaining helps).
- **Milestone 3:** Score at least ~75-80% on OSPF quizzes. OSPF has nuance, so if you miss some, focus on those topics again. Key point: You should be comfortable with reading an OSPF config and understanding what each part does (network statements, router-id, etc.), and interpreting `show ip ospf neighbor/route` outputs. If any output line confuses you, clarify it now (like OSPF route codes: O = intra-area, O IA = interarea, E1/E2 = external – CCNA mostly single area so probably O routes only).
- **Checkpoint:** With OSPF covered, you have tackled the most complex part of CCNA routing. Ensure you also recall earlier routing topics: difference between OSPF and RIP/EIGRP (just basics: OSPF link-state vs RIP distance-vector), but note EIGRP is not in CCNA anymore aside from a mention. Double-check IP Connectivity blueprint: we've done static, OSPF, FHRP. The blueprint also lists understanding *routing table components* and *forwarding decision process*, which we've done. Also, first-hop redundancy (done conceptually). At this stage, you can route within and between networks pretty proficiently! Month 3 is not over – we'll now apply this in context of IP services.

Week 9: IP Services – DHCP, NAT, and Network Services

Objectives (Week 9):
- Understand and configure **DHCP** (Dynamic Host Configuration Protocol) on Cisco devices [96] [97] : both DHCP server (on a router or multilayer switch) and DHCP relay (IP Helper). Know the DHCP process (DORA: Discover, Offer, Request, Ack) and what information is provided (IP, subnet mask, gateway, DNS, etc.).
- Set up **NAT (Network Address Translation)** [98] on a router for IPv4: specifically *PAT (Port Address Translation)* for allowing multiple internal hosts to share one public IP (this is the typical use case). Also know static NAT (one-to-one) usage and configuration. CCNA expects you to configure and verify NAT in IOS.
- Learn about **NTP (Network Time Protocol)** [99] and configure a router or switch to use NTP client mode (sync with a server) and potentially act as NTP server for others. Understand the importance of time sync in networks (for logging, certificates, etc.).
- Cover **SNMP and Syslog** concepts [100] – possibly configuration basics: setting up a SNMP community on a router, and logging to a syslog server. We might not do deep labs on these, but at least know how to verify and the purpose (monitoring, network operations).
- Introduce **QoS basics** (Quality of Service): know what QoS is for – to prioritize certain traffic. Specifically, CCNA might mention classification and marking (DSCP values) and queueing strategies – just theoretical understanding. Possibly see how a router shows QoS config, but configuration likely not required.
- Summarize IP Services domain topics and ensure each is touched: **DNS** (role in network – not config on router, but know it translates names and often there's "ip name-server" command to allow router to resolve names), **FTP/TFTP** uses (for file transfer e.g., router IOS upgrade via TFTP) [101] , and **SSH** configuration on Cisco devices (we did some in earlier labs implicitly, but ensure you can configure a router/switch for SSH access).

Resources:
- *Videos/Tutorials:*
- **"DHCP Configuration on Cisco"** by Keith or Jeremy (YouTube, ~10 min) – demonstrates setting up a DHCP pool on a router and using a relay.

- **Jeremy’s IT Lab Day 19 – DHCP** (YouTube, ~20 min) – likely covers DHCP concepts and a Packet Tracer demo.
- **“NAT Explained + Config”** by NetworkChuck (YouTube, 15 min) – Chuck shows inside/local vs outside/global, typically with coffee shop analogy, then does a PAT config. Good for beginners to catch the idea.
- **Jeremy’s IT Lab Day 20 – NAT** (YouTube, ~30 min) – thorough NAT config demos including static, PAT, verification (`show ip nat translations` etc.).
- **“NTP and Syslog”** (CBT Nuggets or Pluralsight snippet, ~10 min) – explaining how to set timezone, NTP server, and how syslog logging levels work. If not accessible, try a YouTube video on “Configuring NTP on Cisco” (plenty of free ones, ~5 min).
- *(Optional)* **“SNMP Basics”** by Professor Messer (Network+ video, ~5 min) – covers SNMP v2 vs v3 basics and how SNMP is used. Enough for concept.

- *Books/Chapters:*
- **CCNA Cert Guide (Vol. 2)** – It will have chapters on IP Services. Read sections on: DHCP (how to configure a DHCP server on IOS, and DHCP relay agent using `ip helper-address`), NAT (inside/outside concepts, static vs pool vs PAT configuration, and common show commands), NTP (simple client config), DNS (just that a router can be a DNS client or we can use “ip host” to map names, etc.), SNMP (just overview of community strings and basic SNMP operations GET/SET), Syslog (levels 0-7 and how to set logging). QoS likely has a short section – focus on understanding classification, marking (like DSCP), and trust boundaries in a campus (maybe beyond CCNA but just in case).
- **Lab Manual / 31 Days** – likely has a day for NAT and one for DHCP. Go through those for more practice questions.

- **Cisco Press articles** – often there are short guides like “NAT Fundamentals” on Cisco website. Use if you need alternate explanation, especially the NAT address terminology.

- *Research Papers/Articles:*

- **RFC 2131** – DHCP protocol (just read a bit of intro if curious; know it’s UDP 67/68 for exam possibly).
- **Cisco Docs: “Configuring Network Address Translation”** – covers IOS commands and examples for static NAT, PAT, etc.
- **“Troubleshooting NAT”** article – common NAT issues (like not clearing NAT translations after config changes, or forgetting ACL for NAT if needed). Might not be needed if labs go smooth, but good reading.
- **NTP.org brief** – maybe a page explaining NTP strata, but CCNA probably won’t ask that. However, note NTP uses UDP 123, maybe an exam trivial.
- **SNMP vs Syslog** – an article explaining how they differ for network monitoring.

- **QoS Basics** – Cisco has a doc “IP QoS Intro” or search for “DiffServ QoS tutorial” to get the idea of what classification and PHB mean [102] [103] (this correlates to blueprint mentioning PHB for QoS).

- *Online Courses:*

- **Cisco NetAcad – ENSA Modules** likely cover NAT (there’s a known PT lab “Configure PAT”) and DHCP (“DHCP server PT activity”). Do those labs from NetAcad if you have them. They also cover NTP and maybe QoS basics.
- **Skillsoft/Pluralsight** – if you have access, maybe one of their CCNA courses has a quick lab on DHCP and NAT. Not required, but extra perspective if needed.

- **Try HackMe / Packet Tracer mini-games** – not sure if any gamified content for these, but running through config is straightforward enough.

- *Hands-On Labs/Projects:*

- **Lab 9.1: DHCP Server and Relay** – Take a router (or switch) as central and two networks: e.g., Router with two LAN interfaces: one LAN has a router directly connected to PCs, another LAN maybe behind a switch. Configure one router as **DHCP server** for both networks (two pools). For the network where router isn't directly connected (say a router connected to another router which connects to PCs), use DHCP Relay: on that intermediate router interface, configure `ip helper-address <DHCP-server-IP>`. Test from PCs: they should get IPs in correct ranges along with gateway (the router) and DNS if configured. **Expected Outcome:** PC on each network receives valid IP config via DHCP. Use `show ip dhcp binding` on server to verify leases.
- **Lab 9.2: NAT/PAT Configuration** – Create a scenario: Router with an "inside" network (e.g., 192.168.10.0/24 with a couple PCs) and an "outside" network (simulate the internet or a stub network with a server, using, say, 203.0.113.0/24). Configure **PAT** on the router so that all inside addresses can share the router's outside IP. On PCs, set their gateway to the router inside IP. Test by pinging the "internet" server from a PC. It should work if NAT is correctly translating. Do `show ip nat translations` to see the dynamic entries (you'll see inside local, inside global, etc.). Also test something like port translation by maybe using a simulated service if possible, but ping should suffice. Optionally, configure a **static NAT** for one inside host (like make one PC reachable from outside on a static mapping). Try accessing it from the "outside" side. **Expected Outcome:** Internal PCs reach outside resources with NAT functioning, and any static NAT mapping works for inbound.
- **Lab 9.3: NTP and Syslog** – If you have an accessible NTP server (maybe Packet Tracer can simulate one, or use router as NTP master), configure routers to sync time. E.g., one router as NTP master (or actual public NTP if PT supports sending to an address but likely not), others as clients. Use `show clock` to verify time sync. For Syslog, perhaps set up one router as a syslog receiver by using a loopback as the "syslog server" (PT might not simulate an actual syslog server application, but you can at least set `logging <ip>` on devices). At minimum, configure logging host on a router and generate some log (like interface up/down) to see if you get a message (in PT maybe use simulation mode to see syslog packet). If not possible, conceptually ensure you know how to do it.
- **Lab 9.4: SNMP (optional)** – Configure a simple SNMP community on a router (`snmp-server community PUBLIC RO`) and use a PC with a network monitoring tool (PT might not have that) – if not, skip actual test, just know the config.
- **Lab 9.5: End-to-End Network Build** – As a final project for Month 3, build a small company network: 2 departments on separate VLANs (use a switch and router-on-stick or multilayer switch for inter-VLAN), include a DHCP server for clients, use NAT on the edge router to an "ISP", run OSPF on internal routers if multiple. Also implement an ACL (access control list) as a simple firewall to allow internal to outside, but block certain port maybe (we'll do ACL more next week, but you can preview). Essentially, combine multiple technologies into one coherent network. Document the network diagram and configurations as if preparing for a handover to another engineer. **Expected Outcome:** A multi-faceted network that mirrors a simplified enterprise: VLANs, routing (static or OSPF), NAT for internet, DHCP for hosts, etc. This is a synthesis exercise and also good practice for the capstone next month.

- *(Project)* **Documentation and Diagrams:** Take one of your recent labs (like the NAT/DHCP network) and create a professional-looking network diagram using a tool (Lucidchart, draw.io, or even Packet Tracer's drawing tools). Label VLANs, IPs, device names. Write a brief network *documentation* (couple paragraphs) describing the topology and addressing scheme. This practices the soft skill of documentation – very important for a network engineer.

- *Quizzes/Assessments:*

- **DHCP/NAT Quiz:** ~15 questions. Example topics: DHCP message sequence, function of DHCP relay, configuring DHCP pool options (like default-router command), NAT inside vs outside meaning, how PAT differentiates flows (port numbers), identify NAT addresses given a translation (inside local/global definitions), etc. Possibly a scenario: "Host can't get DHCP address – which command is missing?" or "After configuring NAT, inside hosts still can't reach out – what could be wrong?" (like forgot ACL for NAT, or mis-set inside/outside interface).
- **Services Quiz:** ~10 questions covering NTP (purpose, maybe which stratum or which port), SNMP (which version is secure? v3), Syslog (which level is Emergency? difference between level 0 and 7), QoS (maybe one question: "What does QoS classification mean?").
- **Security intro Quiz:** Because next week is Security, maybe preview with a couple of simple Qs now: e.g., "What is the purpose of an ACL?", "Which command enables SSH on a Cisco switch?" (for review if you did it), just to start thinking on security.
- Flashcards: Summarize NAT types, default ports for services (FTP 21, SSH 22, etc – not sure if CCNA requires memorizing many ports, but a handful of common ones is good), syslog levels (0 Emergencies, 7 Debug), SNMP vs Syslog uses, and QoS terms (like congestion avoidance vs congestion management, again maybe beyond CCNA detail).

Time Allocation (~13 hours):
- Videos: ~2 hours (services configs)
- Reading: ~3 hours (multiple small topics to cover)
- Labs: ~6 hours (lots of practical configuration this week)
- Quizzes/Review: ~2 hours (covering various services, which might be lighter individually but many topics)

Milestones & Checkpoints:
- **Milestone 1:** Configure a DHCP server on a router and verify clients get addresses. Show a sample client IP config (from `ipconfig` in PT PC or just show dhcp binding) and ensure gateway/DNS is correctly delivered. If something failed, note how you fixed it (e.g., forgot the `default-router` command initially).
- **Milestone 2:** Implement PAT and demonstrate an inside host reaching an outside host. Use `show ip nat translations` to present one example of a translation (e.g., `192.168.10.5:12345 -> 203.0.113.2:randomPort`). Be able to explain which is inside local/global [104]. If static NAT, show that outside can reach inside using the static mapping.
- **Milestone 3:** Set up NTP in lab or at least configure `ntp server x.x.x.x` on a router. Confirm time sync (maybe use `debug ntp` if possible or `show ntp associations`). If not feasible, state the commands used and expected result.
- **Milestone 4:** Write down in your notes an "IP Services summary" covering DHCP (ports 67/68, DORA), NAT (terms and commands), NTP (basics of client/server), SNMP (v2c vs v3), Syslog (levels 0-7), TFTP/FTP use cases, and SSH vs Telnet difference. This is your cheat-sheet for quick recall.
- **Milestone 5:** Achieve 80%+ combined on the services quizzes. These are straightforward if you labbed – e.g., NAT can be confusing but if you practiced, it's okay. Clarify any missed concept by re-reading that bit of Odom or using device outputs to understand.
- **Checkpoint:** Now the **core network engineering skills are in place** – you've handled network fundamentals, switching, routing, and essential services. The remaining blueprint domains are Security and Automation, which we'll cover in Month 4 and 5, along with lots of review and practice. Reflect on how many configs you can now do: from VLANs to OSPF to NAT. That's huge! Ensure all your lab files

and notes are organized – you might start revisiting them for exam review soon. Take a well-earned break and gear up for Security topics next.

Motivation: Three months down – you're halfway through the timeline and have covered the lion's share of technical topics. It's normal if some things still feel complicated (OSPF or NAT confusions linger), but you have time to refine via reviews and more practice. The key is: **you've built a robust foundation**. In the next months, we'll reinforce it with advanced topics and lots of reviews. Keep pushing forward; you're doing fantastic. Also, maybe start engaging with others (online forums, study groups) to test your knowledge by answering questions – teaching is a great test of mastery. On to Month 4!

Month 4: Security Fundamentals and Advanced Networking

Focus: Month 4 addresses the **Security Fundamentals (15%)** domain and ties up any leftover core topics. We will cover device security (passwords, AAA concepts), Layer 2 security (like port security, DHCP snooping) and wireless security. We'll also introduce some automation basics (to prep for Month 5) and do heavy **review** this month – mock tests and revisiting weak spots. By the end of Month 4, you should have touched all exam topics at least once. **Domains covered:** Security Fundamentals (CCNA 5.0) and parts of Automation/Programmability (basic intro). Plus ongoing review of earlier domains.

Week 10: Device Security and Access Control

Objectives (Week 10):
- Learn about **basic device hardening**: setting strong **passwords** (console, VTY, enable secret) [44], using password policies (minimum length, complexity, etc.) [45], and the importance of disabling unused services. Configure these on a lab router/switch.
- Understand **AAA (Authentication, Authorization, Accounting)** concepts [105]: not configure in depth (that's CCNP), but know that AAA can use local or external (RADIUS/TACACS+ servers). Understand how a Cisco device can use a central server to authenticate admins. Possibly configure a simple local AAA authentication for login as practice.
- Configure **SSH** on a Cisco device: generate RSA keys, set up username/password or AAA, and verify SSH login. Ensure Telnet is disabled (only SSH allowed).
- Implement **Port Security** on a switch [51]: limit MAC addresses on a port (e.g., only allow one MAC and shutdown if violation). Test by connecting a different device to see the violation.
- Implement **ACLs (Access Control Lists)** on a router [50]: Standard ACL vs Extended ACL differences. Practice creating a standard ACL to filter traffic (e.g., block one network from accessing another) and an extended ACL (e.g., permit HTTP but block Telnet). Apply ACLs inbound or outbound on interfaces appropriately and test.
- Understand **ACL best practices** and how they're used for security (basic firewalling) and for control plane (e.g., line VTY ACL to limit who can SSH).
- Cover **Device login banners** (MOTD) for legal warning, and the concept of physical security (briefly).
- This week is heavy on configuration – it solidifies as you do it practically.

Resources:
- *Videos/Tutorials:*
- **Jeremy's IT Lab Day 4 Lab – Basic Device Security** (YouTube, ~10 min) – likely covers setting console/VTY passwords, service password-encryption, etc., which you did partly in Month1 but review now with security lens.
- **Keith Barker "SSH Configuration"** (YouTube, 8 min) – quick steps to enable SSH on a Cisco router/switch.
- **NetworkChuck "Port Security"** (YouTube, 10 min) – demonstration of setting up port security and

showing what happens on violation (with his typical energetic style, possibly caffeinated example).
- **CBT Nuggets "Standard vs Extended ACL"** (if access, ~10 min) – explains the difference and perhaps a scenario of each. Otherwise, try a free video by David Bombal on configuring ACLs.
- **Kevin Wallace "ACL Wildcard Masking"** (YouTube, 5 min) – understanding wildcard masks in ACL (inversion of subnet mask). Many beginners find wildcard confusing, so ensure you get it.
- *(Optional)* **"AAA and RADIUS/TACACS+"** (Network Direction on YT, ~15 min) – to conceptualize AAA. CCNA might only ask e.g., "What is an advantage of TACACS+ over RADIUS?" or "Which port does RADIUS use?" – maybe too deep, but know TACACS+ is Cisco, TCP, encrypts full payload; RADIUS is UDP, encrypts only password. Minor details.

- *Books/Chapters:*
- **CCNA Cert Guide (Vol. 2)** – Read the Security Fundamentals chapter(s). Key topics: securing device access (passwords, SSH), Layer 2 security (port security, DHCP snooping, DAI), basics of VPNs (definition of site-to-site vs remote access) [106], and intro to AAA. Odom likely also covers device monitoring (like SNMP which we did) and an intro to network attacks (DoS, phishing, etc.) – know basic definitions of threats [41] and mitigations. Also read about **ACLs** thoroughly – standard ACL (numbered 1-99 or named), extended ACL (100-199 or named), and where to place them (standard close to destination, extended close to source typically).
- Ensure to cover **Layer 2 security**: Odom will mention *DHCP Snooping, ARP Inspection, Port Security* as in blueprint [52]. Understand what each does: DHCP Snooping prevents rogue DHCP servers; DAI relies on snooping to block fake ARP; Port Security limits MACs to prevent CAM table overflow attacks.
- There might be mention of **WLAN security** here (blueprint has WPA/WPA2/WPA3) – recall from earlier and know the differences (WPA2 uses AES-CCMP, WPA3 adds SAE, etc., but just basics).

- Possibly an overview of **Network Attack types** – e.g., VLAN hopping, spoofing, man-in-the-middle, etc., with mitigations. If present, read to be able to name a few common ones.

- *Research Papers/Articles:*

- **Cisco Guide: "Configuring Secure Management Access"** – covers SSH setup, role-based CLI maybe. Focus on SSH and strong passwords parts.
- **Cisco Port Security Best Practices** – find an article listing recommendations (like stick to one MAC per port for user ports, use violation shutdown).
- **SANS paper on ACLs** – possibly, or just recall from earlier reading.
- **Common threats** – maybe a blog "Top 5 network attacks and how to prevent" to broaden your understanding: e.g., MAC flooding (countered by port security), DHCP spoofing (counter by DHCP Snooping), ARP poisoning (counter by DAI), etc.

- **Cisco Whitepaper: "Network Security Fundamentals"** – if any summary doc exists. Might reinforce CIA triad concept (Confidentiality, Integrity, Availability) – not sure if CCNA explicitly covers that, but could mention if context arises.

- *Online Courses:*

- **Cisco NetAcad – ENSA Module on Network Security**: They have chapters on Access Control, perhaps AAA, VPN overview, etc. Do any Packet Tracer labs on ACLs (there's often a PT "Configure and Verify ACLs").
- **Packet Tracer Activities** – Check PT for pre-made activities like "Port Security" or "Secure Network Device" – sometimes there are.

- **Cybrary/Free Cybersercurity content** – if you want more theory, but for CCNA probably not needed beyond core principles.

- *Hands-On Labs/Projects:*

- **Lab 10.1: Secure Management Config** – Take a lab router/switch, configure: an enable secret, local user account with privilege 15, console login using local, VTY login using local with transport input SSH only, generate RSA keys, and test SSH from a PC. Also set `service password-encryption` (so your line passwords are encrypted in config). Finally, set a login banner (MOTD). **Expected Outcome:** You can only access the device via SSH with the correct user/pass, and console also requires login. The config should show encrypted passwords. Document these steps as if making a checklist (will be useful later).
- **Lab 10.2: Port Security Demo** – On a switch, pick an access port connected to a PC. Configure `switchport port-security` (default allows one MAC) and maybe `violation shutdown`. Connect the PC, see it works. Now disconnect that PC and connect a different device (or change the MAC in PT by replacing the NIC or using another PC). The port should go into err-disable. Check `show port-security interface X` to see the violation count. Then re-enable the port (`shutdown/no shutdown`) and possibly set it to `violation protect` mode to see difference (in protect, won't shut, but drops unknown MAC traffic). **Expected Outcome:** Understanding how port security can block devices beyond the first.
- **Lab 10.3: ACL Practice** – a) **Standard ACL**: On a router with two subnets (A and B), create a standard ACL to block traffic from one specific host or subnet A from reaching subnet B. Apply it inbound on interface toward B. Test with pings: the blocked host should fail, others succeed. b) **Extended ACL**: e.g., block HTTP from one network to a server, but allow other traffic. Use an extended ACL applied appropriately. Alternatively, implement an ACL on VTY lines to allow only a specific IP range to telnet/SSH to the router (for management plane security). **Expected Outcome:** You can write ACL statements (with correct wildcard masks, host vs any keywords) and apply them correctly (right interface, right direction) to achieve desired filtering. Use `show access-lists` to see hit counts after tests.
- **Lab 10.4: Layer 2 Security** – If Packet Tracer supports, try enabling **DHCP Snooping** on a switch (specify trusted ports vs untrusted) and then simulate a rogue DHCP (PT might not easily simulate rogue server, but you can place a second DHCP server in a VLAN and see if snooping blocks it). Similarly, **DAI** needs ARP packets – may skip actual test, but know config. If not feasible, at least review how to enable those (e.g., `ip dhcp snooping` globally and per VLAN).
- **Lab 10.5: Wireless Security** – On a wireless router/AP in PT, try setting different security modes (WEP, WPA2, etc.) to see how a client connects with each. Note how a weak security (like WEP) could be cracked (just conceptually). If possible, show that without knowing passphrase, client can't connect – obvious, but demonstrates necessity of proper Wi-Fi auth.

- *(Project)* **Security Audit Checklist:** Create a checklist for securing a small network device: e.g., "1. Set enable secret, 2. Disable unused ports or put in unused VLAN, 3. Apply port security on access ports, 4. Use SSH not Telnet, 5. Use strong passwords and maybe AAA, 6. Implement ACLs to limit access to network segments, 7. Enable logging and NTP for time sync (for accurate logs), etc." This can be compiled from Cisco best practices. Use this list to verify your own labs have no glaring holes.

- *Quizzes/Assessments:*

- **Device Security Quiz:** ~10 questions – e.g., "Which command encrypts all plaintext passwords in config?" (service password-encryption), "What does AAA stand for?", "What is the default violation mode of port security?" (shutdown), "How many MACs by default if not specified?" (1), etc.

- **ACL Quiz:** ~10 questions – test understanding of wildcards (like "Which wildcard matches 192.168.5.0/255.255.255.0?" answer 0.0.0.255), order of ACL, extended ACL format (src/dst IP and ports), maybe identify what an ACL will do from lines given.
- **Security Concepts Quiz:** ~10 questions – cover general: difference between threat, vulnerability, exploit [41]; VPN types [107] (just definition of site-to-site vs remote-access), wireless security differences, AAA differences (TACACS+ vs RADIUS), maybe one on CIA triad or social engineering.
- **Previous domains mixed quiz:** Add 5-10 questions from routing/switching to keep memory fresh (maybe you can take a small mixed practice test from a site/book).
- Flashcards: Terms to memorize: e.g., "DHCP Snooping – prevents rogue server", "port security default aging: what? (by default secure MAC doesn't age out unless configured)", "Standard ACL range (1-99)", "Extended ACL range (100-199)", "Well-known ports: 20/21 FTP, 22 SSH, 23 Telnet, 53 DNS, 69 TFTP, 80 HTTP, 443 HTTPS, 161 SNMP, etc., to answer any odd question or just to know for ACL port filters)". Also maybe "WPA3 uses SAE (Dragonfly handshake)".

Time Allocation (~13 hours):
- Videos: ~2 hours
- Reading: ~3 hours (security chapters)
- Labs: ~5-6 hours (multiple short config labs)
- Quizzes/Review: ~2 hours

Milestones & Checkpoints:
- **Milestone 1:** Harden a device and verify: e.g., a switch that only allows SSH login with a specific user, and has console secured. Attempt to telnet (should fail), attempt SSH with wrong user (fail), right user (success). If possible, get a peer to try to "break in" (or just simulate by trying defaults) to ensure it's secure.
- **Milestone 2:** Successfully use port security to shut down a port on unauthorized device connection. Check that you know how to bring it back (`errdisable recovery` or manual shut/no shut).
- **Milestone 3:** Implemented ACLs that work as intended. Document one example: "Standard ACL 10 blocking Network X applied on interface G0/0 inbound blocked traffic successfully as shown by ping tests." Also note ACL best practice (like placing, and remember implicit deny at end).
- **Milestone 4:** Quick-fire: be able to answer "How to mitigate X?" for the common threats: e.g., MAC flooding -> Port Security, rogue DHCP -> DHCP Snooping, ARP Poisoning -> DAI, brute-force on device -> strong passwords & login delay, etc. You don't need to know deep, just a one-liner mitigation.
- **Milestone 5:** Achieve ~80% across security quizzes. If there's any term or tech you missed, review it. For instance, if you blanked on "what does SNMPv3 add" (security), just note it down. If ACL logic confused you (like order of lines or implicit deny), clarify with more practice.
- **Checkpoint:** At this point, you have completed an initial pass through **all CCNA domains**. Congrats! You likely have a pile of notes, lab configs, and flashcards. For the remainder of Month 4 and in Month 5, we'll focus on **automation** plus heavy **review and practice exams** to solidify everything. Use this checkpoint to identify your weakest areas – maybe it's OSPF, or ACLs, or subnetting under time. Flag them for extra attention in coming weeks.

Motivation: Security can be detail-heavy, but you've grasped how to lock down a network which is a critical skill. It's satisfying to break and then secure something. Remember, **skills like ACLs and port security are not only exam topics but practical tools** – your future network engineer self will thank you for mastering them now. Keep those study habits strong; you're in the home stretch of content coverage. Month 5 will introduce the final piece (Automation) and then it's all about integrating knowledge and practice tests.

Week 11: Automation & Programmability Fundamentals

Objectives (Week 11):
- Grasp why network **automation** and programmability are emerging: the need for scale, consistency, and integration with DevOps. Understand terms like *SDN (Software-Defined Networking)* [108] – separating control plane and data plane, and *APIs (Application Programming Interfaces)* – how software can interact with network devices.
- Learn about **REST APIs** [109] in the context of networking: e.g., Cisco's RESTful APIs (like those on Cisco DNA Center or even some on IOS-XE). Understand what CRUD means (Create, Read, Update, Delete) [61] and that these map to HTTP verbs (POST, GET, PUT/PATCH, DELETE).
- Get exposure to data formats like **JSON** [65] (JavaScript Object Notation) and maybe XML – CCNA expects you to recognize JSON output and basic structure (key:value pairs, nested). Practice reading a JSON snippet and locating a piece of data (like an IP address in a JSON of interface info).
- Explore **network automation tools**: Know of Puppet, Chef, Ansible (just what they are, not how to use) [63]. Ansible is popular for network automation (YAML playbooks). Puppet/Chef are more used in server world but Cisco wants you aware.
- Basic scripting intro: write a very simple **Python script** to retrieve or configure something, or just parse some output. If you're new to coding, at least understand a provided Python script that uses a library like `netmiko` or requests to call a REST API. We won't become coders in a week, but break the ice.
- Use Cisco's DevNet resources if possible: maybe use the Cisco DevNet sandbox or their always-on sandboxes for DNA Center or CSR1000v API to try a sample API call (alternatively, use Packet Tracer's new REST-based multiuser feature if exists, or just conceptual).
- Tie back to exam: ensure you can answer conceptual Qs like "What is the benefit of controller-based networking?" [110], "What is an example of southbound API vs northbound API?" [58] (Southbound: e.g., OpenFlow, NETCONF; Northbound: REST API to controller). Recognize JSON and interpret it.
- This week is more about reading/understanding than heavy lab, unless you're comfortable to try some coding.

Resources:
- *Videos/Tutorials:*
- **Cisco DevNet "Networking 101: APIs"** (YouTube, ~10 min) – an explanation by Hank Preston or similar about using APIs in network management.
- **NetworkChuck "REST APIs for Beginners"** (YouTube, 15 min) – not network specific, but covers what an API is in simple terms, using maybe a public API example.
- **David Bombal "JSON and Postman for CCNA"** (YouTube, ~20 min) – David often covers new CCNA topics; he may have one showing how to use Postman (an API client) to query a Cisco controller and get JSON data. This could be very practical to watch.
- **"SDN and Controllers"** by Keith Barker (YouTube, ~12 min) – conceptual explanation of SDN and Cisco DNA Center as an example, plus traditional vs SDN differences.
- **CBT Nuggets "Automation and Programmability Basics"** (if access) – might have a high-level video summarizing these emerging tech within CCNA scope.
- *(Optional)* **"Python for Network Engineers Crash"** (YouTube, e.g., by Kirk Byers or others, 1 hour or more) – only if you have time/interest to go deeper. Focus on simpler: how to open a SSH connection with netmiko, or parse an IP from a text using Python regex. But that may be beyond what's needed.

- *Books/Chapters:*
- **CCNA Cert Guide (Vol. 2)** – The last chapter(s) on Automation & Programmability. Read all sections: Network Architectures (controller-based vs traditional), APIs (northbound/southbound), configuration management tools (just understand they manage configs and ensure desired

state), Cisco DNA Center & SD-Access overview (fabric, overlay/underlay concepts from blueprint) [108], JSON data format (they might show an example and point out how to pick values) [65].

- There might also be mention of model-driven programmability (YANG models, NETCONF) – just note those words, maybe one exam Q.
- **Cisco DevNet Assoc. book** (if any excerpt is available) – might have overlapping content with CCNA automation section for deeper interest.

- **Appendix or Additional Reading:** Odom might reference some DevNet resources; check if any recommended reading on JSON or APIs.

- *Research Papers/Articles:*

- **Cisco Whitepaper: "Intent-Based Networking"** – describes concept behind controllers like DNA Center (which uses intent-based policies). Good to get buzzwords like "intent, automation, assurance".
- **Blog: "APIs for Network Engineers"** – a blog by a network engineer who learned Python, explaining how they use REST APIs to get device info.
- **JSON tutorial** – lots online, but maybe an interactive one where you view a JSON example. If not, even Wikipedia JSON page shows an example to interpret.
- **DevNet "Hello Network!" lab** – if you register on Cisco DevNet (free), they have some guided labs on using sandbox. Maybe try "REST API Basics" or "Always-On Sandbox demo".
- **OpenFlow overview** – just read what OpenFlow is historically (protocol for controllers to program switches – used in early SDN, now not as talked, but part of history).

- **Terraform/Chef/Puppet** – no need detail, just know these are Infrastructure as Code (IaC) tools, beyond CCNA likely.

- *Online Courses:*

- **Cisco NetAcad – DevNet Associate course** (if available, not sure if free). If accessible, might have beginner labs on using Postman to query Cisco DNA.
- **Postman or curl practice**: If you have access to a network device with API (maybe PT doesn't have, but you could install Cisco Packet Tracer and see if it supports some API?), alternative: use a dummy public API (like a weather API) in Postman just to get comfortable with GET/POST and see JSON.

- **Coding practice**: if new to Python, perhaps use an interactive site like Codecademy for a couple of Python lessons just so you can read code. But time is short; if you already code a bit, maybe attempt something small like using Python to read a JSON file.

- *Hands-On Labs/Projects:*

- **Lab 11.1: Explore a REST API** – Use a tool like Postman (install on your computer) or Python `requests` library to GET data from an API. If you don't have a Cisco device API, use something like httpbin or a dummy JSON API. Alternatively, many Cisco devices have an HTTP interface you could enable (not secure, but for test). If you can, enable REST API on a DevNet sandbox or CSR1000v VM (this might be advanced – if not, skip doing it yourself). At least, open a sample JSON file (maybe Odom's book has one, or find on DevNet) and try to pick out key info. **Expected Outcome:** You understand how an API call returns structured data (JSON) and how it differs from CLI show output.

- **Lab 11.2: Simple Python Script** – Write or copy a short script that does something like “print all IP addresses in this JSON” or “SSH to router and run show ip int brief (using netmiko)”. If you’ve never coded, ask a programmer friend or find a ready script from DevNet Code Exchange. Running it successfully and seeing output is the goal. If not comfortable, at least go through the thought: how would automation save time vs manual CLI (imagine configuring 100 VLANs on 10 switches – script can do it faster with less error).
- **Lab 11.3: Controller Demo** – If possible, watch a demo or recording of Cisco DNA Center or Packet Tracer’s SDN Controller (PT has a “Controller” object for SDN but not sure how functional). At least conceptually: one central controller can push VLAN configs to all switches or do dynamic path optimization. Recognize how this differs from logging individually.
- **Lab 11.4: JSON Parsing Exercise** – Create a small JSON structure (or use sample) that includes network info, e.g.: `{"interface": "Gig0/1", "ip_address": "10.0.0.1", "status": "up"}`. Write down how you’d access the IP address field (answer: by key "ip_address"). Maybe test with a Python one-liner if possible: `import json; data=json.loads(<jsonstring>); print(data["interface"])` to print values. **Expected Outcome:** Not to memorize syntax but to demystify JSON (it’s just text with keys/values, often easier than parsing CLI output).

- *(Project)* **Automation Strategy Proposal:** Imagine you manage 50 switches – list 3 tasks you would script/automate (e.g., backup configs nightly, bulk update SNMP community, verify interfaces up). For each, describe how automation helps (less error, schedule it, etc.). This isn’t on exam, but thinking this way prepares you for real network engineering in modern environments and gives context to why Cisco added this domain.

- *Quizzes/Assessments:*

- **Automation Concepts Quiz:** ~10-15 questions. Cover north vs southbound API, e.g., “Which is a southbound API? a) REST to DNA Center, b) NETCONF to routers, c) web dashboard GUI (northbound example).” Ask about benefits of automation (fewer errors, consistency, speed). Maybe “Which data format is easiest for machines to parse? JSON vs XML vs YAML – arguably JSON/YAML both fine, but JSON is ubiquitous). Some basic Python logic like “which of these is a correct list syntax in Python?” or maybe not – CCNA not a coding test but might have pseudo-code trace (but rarely). If any question, likely identify JSON vs XML or a Python snippet output. For instance, they may show a JSON and ask “what is the value of X key?” – test if you can read JSON. Or a Python `print(data["ip"])` and ask what it does (print the value of "ip" key from data dictionary). If you’ve done above exercises, you’d get it.
- **DevOps Tool Quiz:** ~5 questions – maybe matching “Puppet/Chef” to “uses declarative manifests and agent on nodes” vs “Ansible uses SSH, agentless, uses YAML playbooks” vs “SaltStack, etc.” If CCNA doesn’t go deep, maybe one question: “Which tool uses a push model? (Ansible) vs pull model (Puppet)”. But likely just identify these as automation/config management tools.
- **Full-length Practice Exam #1:** This is a good point to take a **full CCNA practice exam** (60-70 questions, 2 hours). Use Boson ExSim if you have it (highly recommended [111] [112]) or the Cisco Official Practice if available, or a free one (ExamTopics – but caution, verify answers). Simulate exam conditions: 120 min timer, no notes. Afterward, grade and *analyze every question*, especially the ones you got wrong or guessed. This will highlight any weak areas to focus on in Week 12 and Month 5 review.
- Continue Flashcards: add any new ones (like “API = Application Programming Interface, allows software to communicate via defined requests”, “CRUD = Create,Read,Update,Delete”, sample JSON syntax). Also maybe flashcard any facts you got wrong in practice exam. By now, flashcards should be a sizable deck – keep doing daily reviews; it’s a great retention tool up to exam day.

Time Allocation (~12 hours):
- Videos: ~2 hours
- Reading/learning: ~3 hours
- Hands-on (if doing script/API calls): ~3 hours (maybe more if really diving, adjust as needed)
- Practice Exam and review: ~4 hours (2h exam, 2h review)

Milestones & Checkpoints:
- **Milestone 1:** Write a short explanation (4-5 sentences) of the difference between traditional networking vs controller-based. E.g., "Traditional: each device configured individually (CLI), control plane distributed; Controller-based: central brain (controller) tells devices how to forward, devices are simpler, easier to enforce policies network-wide." If you can articulate that, you got the core idea [110].
- **Milestone 2:** Interpret a given JSON. For instance, take: `{"device": {"name": "R1", "interfaces": [{"name": "Gig0/0", "ip":"10.0.0.1"}, {"name":"Gig0/1","ip":"10.0.1.1"}]}}`. Answer: how many interfaces does R1 have and what are their IPs? (Should be: 2 interfaces, IPs 10.0.0.1 and 10.0.1.1). If you can do that, you're good for JSON interpretation [65].
- **Milestone 3:** (Optional but cool) Successfully run a simple network automation action – whether it's an API GET retrieving something or using a script to login and run a command. If accomplished, celebrate – you've stepped into netprog! If not, at least know what such a script would generally look like.
- **Milestone 4:** Complete the full practice exam and identify improvement areas. Suppose you scored, say, 70% – not bad for first full attempt; list which sections had wrong answers. Make a plan to review those (which we'll do Week 12 and Month 5). If you scored 90% – great, but still review any misses and note if it was luck on some guesses; ensure those are solidified.
- **Checkpoint:** Content learning phase is nearly done. All topics are covered. The focus shifts to **reinforcing knowledge, practicing scenarios, and test readiness**. Compare where you were at Month 1 vs now – impressive progress, right? The next step: refine until you're consistently exam-ready and confident in practical skills too. Use Month 5 for that polishing, plus a capstone project to apply everything.

Motivation: Automation is a new frontier – don't worry if you felt like a newbie again here. The CCNA only dips a toe into programmability; mastery comes with practice over time. The key takeaway is you now know *what's possible* and won't be intimidated by terms like JSON or API in the field. Embrace a growth mindset – network engineering is evolving and so are you. Now, let's gear up for the final phase: intense review, practice tests, and a big capstone lab to ensure you're more than ready for the exam and the job market.

Week 12: Comprehensive Review and Mock Exam

Objectives (Week 12):
- **Systematic review** of all domains: Each day of this week, focus on one domain's key points and "must-know" facts/configs. E.g., Day1: Network Fundamentals recap, Day2: Network Access recap, etc. Use your notes, flashcards, and maybe re-watch 2x speed videos or skim chapters to reinforce.
- Identify and fill any remaining gaps: If certain labs were skipped or still shaky (maybe IPv6 or OSPF area type details), address them now with quick labs or reading.
- Take at least one more **full-length mock exam** (preferably a different set of questions than week 11's). Aim to exceed the passing score margin (target ~90% so you have cushion).
- Practice **Simulations and practical scenarios**: If you have access to simulation-style questions (like configuring something under time), practice a couple. If not, create your own mini-scenarios to configure without looking at guides (like: "Configure OSPF on these routers, with passive interface on LAN, and default route advertisement – go!" and see if you can do it quickly).
- Refine test-taking strategies: manage time (approx 1 min/question, more for sim), flag tough

questions and move on, eliminate wrong answers in MCQs by logic, etc. Train your brain to stay calm and methodical during the exam.
- Ensure you are ready with practical skills as well: though CCNA is theory + some sim, for job readiness, ensure you can do the common tasks without peeking at notes now.
- By end of week, be exam-ready and also ready to apply knowledge in a capstone project next month.

Resources:
- *Videos:*
- Watch any “Last minute CCNA review” videos (there are often 1-2 hour marathon reviews on YouTube summarizing key points). E.g., “CCNA in 120 minutes” type videos – good for high-level catch-all revision.
- **Exam tips videos** (many CCNA mentors have “tips to pass” with advice on question wording, how to not overthink, etc.). This might ease anxiety and give insight on Cisco’s style.
- If certain topics still fuzzy, revisit those specific video sections at higher speed for clarity.

- *Reading:*
- Skim through your compiled notes and highlight anything you’d hesitate on if asked outright. If you find any, clarify immediately (look up that detail).
- Re-read the exam blueprint list we compiled at the beginning. Can you give a sentence or two about each sub-bullet if asked? If not, review those.

- If you have the Odom books, the end-of-book “Key Topics” and “Do I Know This Already” quizzes are excellent for quick review. Use those as a checklist.

- *Practice exams:*

- Boson ExSim – do Exam B (if you did A earlier) under exam conditions. Review thoroughly.
- Pearson/Cisco Official Practice exam (if you have it).
- Take some free online quizzes for variety (careful with brain dump sites; better use reputable ones like Todd Lammle’s site or others with practice Qs).

- If scoring consistently ~85%+, that’s a good sign. If below ~80%, identify why – content gap or tricky wording? Fix content gaps and practice interpreting wording (dissect what the question really asks).

- *Lab practice:*

- Quickly lab any config that you don’t feel second-nature: e.g., “Setting up trunk + EtherChannel” quickly, or “One static NAT and one PAT” quickly. This just builds muscle memory and confidence.
- If possible, do a timed lab: e.g., give yourself 30 minutes to configure a small network from scratch (3 routers OSPF + 2 VLANs + NAT, etc.). This isn’t for exam (they won’t be that extensive due to time), but for you to consolidate integration of topics.

- Ensure you know how to verify and troubleshoot in labs swiftly: e.g., commands like `ping`, `traceroute`, `show ip int brief`, `show cdp neighbors`, etc., should come to mind easily to diagnose things, because some exam sims might require troubleshooting a misconfig.

- *Flashcards:*

- By now you have many flashcards – keep reviewing daily, but also start trimming ones you always get right (or mark them as known). Focus on ones you still slip on.

- The day before exam (in plan, that's next month), you might just skim through all to ensure nothing forgotten.

- *Health/Mental Prep:*

- This is part of review week too: Plan your exam logistics (if you intend to take it right after Month 5, schedule it now so you have a date [71] !). Having it scheduled will drive you.
- Ensure you get good rest and not burn out this week – if you study too hard without breaks, retention drops. Take short breaks, stay hydrated, exercise a bit.
- Practice some mindfulness or positive visualization: imagine opening your exam result with a pass – that's motivating and calms nerves.

Milestones & Checkpoints:
- **Milestone 1:** Score well on Mock Exam(s). For instance, if Boson exam gives scores per section, ensure none of the six domains is below ~80%. If one is, revisit that domain's content until you can raise it.
- **Milestone 2:** Conduct a thorough **self-assessment**: Print out (or write down) each exam blueprint topic and rate your confidence 1-5. For any 3 or below, do a targeted review. After review, all should be 4 or 5 (meaning "I could answer an exam question or do a basic lab on this").
- **Milestone 3:** Complete a final lab or troubleshoot challenge without hints, successfully. For example, purposely break something in a network (like an OSPF area mismatch or an ACL blocking a service) and see if you can find and fix it quickly. This shows you can apply knowledge dynamically, which is great for job skills.
- **Milestone 4:** Organize your study materials for next month's capstone and job prep: e.g., have your best notes and diagrams ready to refer to when designing the final project and for interview prep (it's handy to show or at least talk about a project with documentation).
- **Checkpoint:** You should now feel *ready to schedule or soon take the CCNA exam*. If not, identify what's holding you back – content, test anxiety, etc. This plan assumed exam after 6 months; if you're ahead of schedule and feel ready now, you could even take it earlier. If not, adjust plan to do more practice where needed. The key is mastery and confidence.

Motivation: You are basically at the summit of CCNA preparation. The view is great – look back at all the concepts you've mastered! This week's intense review might be tiring, but think of it as polishing a gem: you're refining rough edges so you can shine on exam day. Keep the momentum but also start envisioning life post-exam (the next section will help with that – job prep, etc.). Remember, **the goal is not just to pass an exam, but to become a capable network engineer**, and you're well on your way.

Month 5: Final Prep, Capstone Project, and Exam Readiness

Focus: Month 5 is about **consolidation and application**. We will integrate everything in a realistic **capstone project**, do last-mile prep with mock exams and flashcards, and finally take (and pass!) the CCNA exam likely in Week 4 or end of this month. Post-exam, we'll transition to job preparation tasks. (If you plan to take the exam in Month 6 instead, you can adjust accordingly, but this plan assumes by end of Month 5 you attempt the exam).

Week 13: Capstone Network Design Project – Plan

Objectives (Week 13):
- Begin a **capstone project**: designing a small enterprise network from scratch, incorporating most technologies learned. This week, focus on planning and design on "paper" (or software) before implementation next week.
- **Scenario:** You are tasked to design a network for a small company with, say, 3 departments (like

Admin, Engineering, Sales), two sites (HQ and Branch), and internet connectivity. They require: VLANs per department, inter-site routing, internet access for all via HQ, secure remote access for a few employees (VPN), and basic network security measures.
- Create a **network diagram** of this topology: likely includes routers at each site, switches, maybe a firewall (optional, or use router ACL as firewall), an ISP cloud, and maybe a server network.
- Plan IP addressing: assign subnets to each VLAN and site, ensuring summarization if possible and avoiding overlaps. Perhaps use private IPs internally and one public range for NAT at HQ.
- Choose and justify routing: e.g., use OSPF between sites (maybe over a simulated WAN), static default to internet, etc. - Plan out where to apply security: e.g., port security on user ports, ACL on router to filter internet traffic, VPN using perhaps Packet Tracer's VPN feature (if any, else just conceptual).
- Essentially, **write a network design document**: including network requirements, IP scheme, device roles, protocols, and security measures.
- Get feedback if possible: if you have a mentor or friend in networking, show them the design for critique. If not, self-review by comparing to reference architectures from Cisco (e.g., Enterprise Network Model).

Resources:
- *Reference Designs:*
- Cisco Validated Designs or CCNA case studies. Perhaps Cisco Press CCNA books had a final chapter with a case study network – use that as inspiration or reference.
- The old "Hierarchical Network Model" (Core/Dist/Access) – since we have HQ and Branch, maybe HQ has a core switch and some access switches. Use two-tier design (collapsed core) given small size.
- **Subnet calculators** (to double-check your addressing plan efficiency).
- **Visio or draw.io stencils** – for making a nice diagram. (Or Packet Tracer's built-in drawing for a quick visual).

- *Design considerations:*
- VLAN for each department (plus maybe a management VLAN, and a VLAN for voice if any VoIP – optional).
- Redundancy: maybe not a huge network, but could have two switches at HQ with EtherChannel and HSRP for gateway redundancy as a bonus. If it complicates, keep it smaller.
- Branch could be simpler (one router, one switch).
- WAN link: simulate maybe as a serial or just an IP cloud. If using PT, can connect routers via cloud or directly.
- Security: plan where to put an ACL (likely on HQ router outbound to internet to restrict certain traffic, and inbound from internet to allow only VPN or necessary).
- VPN: If PT supports GRE or IPsec, perhaps plan an IPsec tunnel between HQ and Branch or for remote user – if not, just state it.
- Automation: not required in design, but you can mention future plan to use Ansible for consistency.

Milestones & Checkpoints:
- **Milestone 1:** Complete a **network diagram** of the proposed design, showing all subnets and VLAN IDs, device names, interfaces, and relevant IP addresses. This is the blueprint for your implementation.
- **Milestone 2:** Write out the **IP addressing plan**: e.g., "192.168.10.0/24 – Admin VLAN 10 at HQ (50 users), 192.168.20.0/24 – Eng VLAN 20 at HQ (30 users), 192.168.30.0/24 – Sales VLAN 30 at HQ (20 users), 192.168.40.0/24 – Branch office LAN (30 users). WAN: 10.0.0.0/30 between HQ and Branch." Ensure the sizing fits (no VLAN has more IPs than needed but leave some growth).
- **Milestone 3:** Enumerate the technologies to use: "OSPF area 0 between HQ and Branch routers; Inter-VLAN routing via multilayer switch at HQ or router-on-a-stick; PAT on HQ router for internet; Port security on access ports (max 2 MAC for phones+PC maybe); DHCP from HQ server/router; ACL on HQ

router to block certain ports (e.g., disallow telnet from outside); Site-to-site VPN planned (conceptual).” This list will guide config.
- **Checkpoint:** Validate the plan against CCNA topics: did you include at least something from each domain? Likely yes: VLANs (Network Access), OSPF (IP Connectivity), NAT/DHCP (IP Services), ACL/security (Security Fundamentals), maybe mention of automation (like “we will use SSH and maybe network scripts for config backup” for Automation, albeit light). The aim is to demonstrate holistic understanding.
- Next step will be implementing and testing this design in Week 14.

Motivation: Designing a network from scratch is the ultimate test of understanding – it forces you to consider how pieces fit together. Don’t worry if you have to adjust along the way (that’s normal). Enjoy this creative and analytical process – it resembles real job tasks. You’re effectively acting as a network engineer/architect now, which is exactly the outcome we wanted. Take pride in that!

Week 14: Capstone Network Implementation and Test

Objectives (Week 14):
- Implement the designed network in Packet Tracer (or real gear if accessible) step-by-step.
- Configure VLANs and trunking at HQ, set up inter-VLAN routing (either a layer 3 switch SVIs or a router-on-a-stick). Configure OSPF between HQ and Branch routers, ensure routes exchanged.
- Set up DHCP server (maybe at HQ for all subnets, using DHCP relay to branch). Set up NAT on HQ for internet access simulation (use a loopback or cloud as Internet).
- Apply security: port security on switches, ACL on HQ router for traffic filtering, secure device configs (SSH login). If possible, configure an IPsec VPN between HQ and Branch (PT might have a “VPN easy” option on routers – if not, simulate by just allowing direct since it’s lab).
- Test end-to-end: from a PC in each VLAN, ping others, ping branch, ping internet (maybe simulate internet as a server in a different network beyond HQ router). Test fail-safes if any (e.g., if you did HSRP with two routers at HQ, shut one to see continuity).
- Troubleshoot any issues encountered – this is likely. It’s part of learning: maybe OSPF adjacency fails due to passive interface or NAT issues. Work through them systematically (like you would on exam sims or real world).
- Once stable, **document the configuration**: save config files, and perhaps write an executive summary of the network to accompany the diagram.
- This project is also material you can mention in interviews or on a resume (it’s home lab, but it shows initiative and skills).

Resources:
- *Packet Tracer*: Use PT’s multi-tab to keep track of different config sections (and it allows notes on topology).
- *Prior labs*: You basically will reuse many configurations from prior weeks but combined. Refer back if needed (no shame in checking a command if memory is unsure – in real world you’d check docs – but try to recall first).
- *Peer review*: if you know someone else in CCNA, maybe share your Packet Tracer file for them to test, and vice versa. Fresh eyes might catch config mistakes.

Milestones & Checkpoints:
- **Milestone 1:** All critical configs done: VLANs, OSPF, NAT, DHCP, ACLs, port security. The network should be functioning as intended. For example: Users get IP via DHCP, can reach resources in other VLANs and branch, internet pings go out (maybe not real internet but a fake server), and disallowed traffic is indeed blocked by ACL.
- **Milestone 2:** Testing results documented. Make a table: each VLAN PC -> where should it reach and

not reach? Test ping/HTTP etc. E.g., "PC in Sales VLAN -> should reach Branch server (ping ok), should browse internet (http ok, tested by HTTP to fake server), should NOT telnet outside (tried telnet, blocked as expected by ACL)." Do this for key scenarios. All tests should align with design goals.
- **Milestone 3:** Configuration review: run `show run` on each device and ensure no glaring issues (e.g., default passwords, missing service encryption, etc.). Also note resource usage: Did you use small subnets efficiently? Are there any routing table oddities? Clean up if necessary (like remove any test ACL lines, etc.).
- **Milestone 4:** Save your final Packet Tracer file and also export configs (for your portfolio). Create a brief **Network Implementation Report** with the diagram, summary of addressing, summary of protocols, and verification outputs (like OSPF neighbor table, NAT translation sample, etc.). Even if just for yourself, this consolidates what you've built.
- **Checkpoint:** Congratulate yourself – you've essentially simulated the job of setting up an enterprise network! This capstone ties together months of learning. It should boost your confidence that not only can you answer exam questions, you can actually apply the knowledge. This is the bridge from certification to real-world skill. Use this accomplishment as a talking point in interviews and as personal validation of your abilities.

Motivation: Finishing a project like this is hugely satisfying. Think about how far you've come – from not knowing what a VLAN or OSPF was, to now building a network with both. That's tangible progress. If parts of the project were challenging, that's good – better to face challenges in practice than in production. Now, any remaining focus can shift fully to exam-day readiness and job prep, knowing that your skill foundation is strong.

Week 15: Final CCNA Exam Preparation and Rest

Objectives (Week 15):
- **Final exam prep**: do a last round of practice exams or question banks focusing on weak areas identified. If you have Boson Exam C or other sets, do them.
- Review flashcards or notes for anything that still trips you up. At this stage, avoid overloading on new info; just solidify recall and understanding.
- Go over **exam-day logistics**: Ensure you know location if in-person, or setup if online (test your webcam, internet, clear workspace if doing online proctored). Have two forms of ID ready. Read PearsonVue exam rules.
- Prepare mentally: in the last 1-2 days before exam, shift to light review and **adequate rest**. You won't gain much new knowledge cramming last minute, but you could tire yourself. Better to be fresh.
- Maybe skim through the official exam topics list one more time and say out loud or on paper the main concept of each – if those come easily, you're set.
- Plan to **arrive early** if going to a center, or be set up early if online.
- Have a strategy: e.g., initial 10 seconds brain-dump on scratch paper (some do this for subnet table or key acronyms – though some test centers might not allow writing until exam starts, check rules).
- Confidence: remind yourself of all the work put in. Some anxiety is normal, but trust your preparation. You have consistently scored well in mocks by now and the capstone success shows deep understanding.
- **Exam Day:** Execute your plan calmly. Manage time – if a question is super confusing or long, mark and move on, come back if time. Many find they have extra time at end because they practiced pacing. Use any leftover time to review flagged questions.
- After submitting, breathe – you'll see the result on screen. We expect a **PASS!** If for some reason not (stuff happens), analyze and you still have Month 6 to re-focus – but likely you got it.
- Celebrate achievement – it's huge. Then short break and onward to job hunting prep.

Resources:
- *Test-Day tips articles* – e.g., “What to do on CCNA exam day” blogs, often recommending good sleep, light meal, etc.
- *Pearson Vue tutorial* – if you can find a preview of the exam interface (sometimes they have a generic test tutorial), to know how sim questions look and how to answer drag-and-drop etc.
- *Online communities* – some people post their exam experience (without violating NDA). It can be reassuring to read a few “I passed CCNA, it was easier/harder than I thought” just to calibrate expectations, but don't let it spook you – everyone’s experience varies.
- *Your support system* – whether friends or family, let them know you have the exam and maybe arrange something fun after as a reward.

Milestones & Checkpoints:
- **Milestone 1:** Achieve passing scores on final practice tests consistently (~85%+). If any domain still lingers in 60-70%, do targeted quick refresh (e.g., re-read that chapter summary or watch a short video) until you’re confident.
- **Milestone 2:** Flashcards all green – by now, you might retire the deck, or just quickly flip through and realize you know it all. If a few sticky points remain (like memorizing some numeric values or IEEE numbers, etc.), decide if it’s worth last-minute memorizing. CCNA is more about understanding than rote memorization (apart from subnetting maybe), so focus accordingly.
- **Milestone 3: Exam completed with passing score.** You’ll get a preliminary pass notification. Huge moment! You can now proudly call yourself a Cisco Certified Network Associate. This is the culmination of the 5 months of hard work.
- **Checkpoint:** With the exam behind you (hopefully), shift mind to leveraging this cert: updating resume, sharing the news on LinkedIn, and preparing for job interviews. The final month will focus on that transition.

Motivation: This week is about keeping a cool head and trusting your journey. Confidence is earned, and you’ve earned it. Imagine walking out of the testing center with a grin, or seeing “Congratulations!” on the screen. It’s not luck – it’s your dedication paying off. And remember, even beyond the exam, the knowledge stays with you. As the CCNA motto suggests, it’s not just a test, it’s training for your career. Go get that cert!

Month 6: Post-CCNA Career Preparation

Focus: With CCNA in hand, time to land that job! Month 6 (which might start immediately after passing or overlap if you took exam in Month 5) is devoted to job search prep: polishing resume, practicing interview questions (technical and HR), labbing any practical skills for interviews, and continuing to learn (perhaps start looking at CCNA specialization or CCNP topics lightly, to discuss future plans in interviews).

We’ll break it into 4 weeks with tasks, but you can adjust based on your situation (you might already be in a job and just need to leverage CCNA for promotion, etc.). We assume you’re seeking a network engineer role or NOC/helpdesk that values CCNA.

Week 16: Update Resume and Online Presence

Objectives (Week 16):
- Update your **resume/CV**: Highlight the CCNA certification (and mention knowledge of specific skills from it). Also add any hands-on projects (like the capstone you did, home lab setups). Emphasize practical skills: e.g., “Configured and managed VLANs, OSPF routing, and ACLs in lab environments.”

- If you have prior IT experience (even in helpdesk), tailor it to show networking exposure or relevant problem-solving.
- Keep resume concise (1-2 pages), focus on skills and achievements. Possibly add a lab section or personal projects section, since as a beginner that shows initiative.
- Create or update your **LinkedIn**: add CCNA cert (you can add via Cisco's Cert manager to verify). Write a bio that you are a certified network engineer excited about networking. Connect with people (recruiters, network engineers, people from local Cisco user groups).
- Clean up your online presence (if any professional footprint beyond LinkedIn) – ensure your LinkedIn photo is professional, and no inappropriate public posts elsewhere that employers might see.
- Consider creating a **portfolio** site or GitHub: maybe upload some sanitized lab configs or documentation, or a blog post about your study journey. This isn't required, but can set you apart if you enjoy writing or sharing knowledge.
- Have someone review your resume (a mentor, friend in industry, or even use a free online resume critique service if available). Feedback ensures it's clear and impactful.

Resources:
- *Resume templates* – find a clean, modern template if you want a refresh. Avoid overly fancy graphics; ATS (applicant tracking systems) prefer straightforward formatting.
- *LinkedIn examples* – look at profiles of other CCNAs or entry-level network engineers to see how they present themselves.
- Cisco's **Talent Network** – maybe sign up or see what they list as desired skills; incorporate keywords (like "Cisco routers, switching, troubleshooting, TCP/IP, etc.") into your resume so automated filters catch them.
- *Professional photo* – if you don't have one, have someone take a clear headshot of you in business casual.
- *Cert verification* – Cisco has a verification tool; you may get a PDF certificate and ID – mention the ID on resume or just say "Cisco Certified Network Associate (CCNA), attained [Month Year]".

Milestones:
- **Milestone 1:** Finalize resume with CCNA included and at least one project/experience bullet demonstrating networking skills. E.g., "Built a multi-site network in lab using OSPF and implemented network security (ACLs, VPN)" – this is from your capstone. Even if lab, it's relevant experience.
- **Milestone 2:** Update LinkedIn profile to "Open to work" (if job hunting) and with CCNA credential. Post an update about achieving CCNA – often that can get attention from connections and maybe recruiters (plus congrats that make you visible).
- **Milestone 3:** Ensure other sections are good: short summary in resume emphasizing you are eager to apply networking knowledge, education updated (if you did any courses, mention Networking Academy courses or self-study).
- **Checkpoint:** You now have a professional presentation to the world as a network engineer. Next, we'll focus on preparing to deliver in interviews and assessments.

Motivation: Marketing yourself might feel different from technical study, but it's crucial. You earned a valuable cert; don't be shy to show it off in a polished way. A strong resume and LinkedIn can open doors. Think of it as configuring yourself as the network device now – optimized for discovery by recruiters!

Week 17: Common Interview Questions and Lab Drills

Objectives (Week 17):
- Prepare for **technical interview questions**: these could be theoretical ("Explain OSPF vs RIP"), scenario-based ("If a user can't reach Google, how do you troubleshoot?"), or simple direct questions

(“What is a VLAN? What is subnetting and why is it useful? Describe the TCP handshake.”).
- Compile a list of ~20 common networking interview questions (Google “CCNA interview questions”). Write out or speak your answers, ensuring clarity and confidence.
- Particularly focus on areas interviewers love: subnetting on the fly (they may ask you to calculate a subnet or find a subnet ID quickly), troubleshooting approach, and basic definitions.
- Practice **behavioral questions** too (STAR method: Situation, Task, Action, Result): e.g., “Tell me about a time you solved a difficult technical problem” – you can use your labs or projects as examples (“I was configuring OSPF and neighbors wouldn’t form; I systematically checked parameters, found a mismatch, resolved it – showing persistence and troubleshooting skills”).
- If possible, do a **mock interview**: have a friend pose as interviewer (preferably someone in IT) and run through questions. Or record yourself answering and critically review (are you concise? Too nervous? Using filler words?).
- Brush up on any tool or platform mentioned in job listings: e.g., some places might use Ticket systems (like ServiceNow) – be ready to say you are familiar with the concept of ticketing; mention documentation skills (like using Notion or wiki as you did for notes).
- Revisit labs to ensure you can do simple tasks if asked on spot (some interviews might have a practical test, like configuring a switch or writing an ACL). If you have access to Packet Tracer during an interview or whiteboard, practice explaining your steps as you would if they watch you configure.

Resources:
- *Interview question lists:* Many blogs and YouTube videos list top CCNA or network engineer interview questions. E.g., “What is the difference between a hub, switch, and router?”, “How does traceroute work?”, “What is ARP?”, “Describe an IP routing process.”
- *Glassdoor* – search for network engineer interviews at companies to see real questions they got.
- *Mock interview services* – if you want professional help, some platforms connect you with industry pros for mock interviews (sometimes paid).
- *Friends or mentors* – if you know someone in networking, ask if they’d quiz you. They might throw in curveballs which is good practice.
- *Technical practice:* If expecting a technical test, review how to configure basics quickly. Possibly set a timer for yourself to, say, assign IPs to interfaces and get OSPF running in 10 minutes. Speed isn’t usually tested in interviews deeply, but you want to show you know your stuff without too much guess.

Milestones:
- **Milestone 1:** Create an Q&A list with answers you're happy with for at least 20 likely technical questions. For example, Q: “What’s the difference between TCP and UDP?” – A: “TCP is connection-oriented, provides reliable delivery with acknowledgments and retransmission, used for things like web browsing; UDP is connectionless, no guarantee of delivery, used for streaming or DNS where speed is important.” Practice saying it aloud smoothly.
- **Milestone 2:** Successfully perform a mock troubleshooting scenario. E.g., friend says: “User can’t access email.” You verbally walk through troubleshooting: “First, I’d ask if others are affected (scope). Then check connectivity: ping user’s PC, gateway, etc. Check DNS if webmail. If network, could be an ACL or route issue…” – show logical approach. The goal is to demonstrate you have a structured method, not necessarily solve an unknown issue in real-time (they want to see your thinking).
- **Milestone 3:** Identify any weak points that came up during practice. Perhaps you stumbled explaining STP or forgot part of the OSI model. Quickly brush up on those now.
- **Checkpoint:** By now, answering typical interview questions should feel much easier than before your studies. You can talk about technologies confidently and also showcase critical thinking in troubleshooting. This is crucial for convincing employers. Next, we’ll target job search and refining such communication further.

Motivation: Remember, an interview is as much about **demonstrating your enthusiasm and thought process** as it is about reciting facts. Given your preparation, you *know* the facts – now convey your passion for networking and your problem-solving skills. Every question is an opportunity to show you're not just certified, but also a great colleague to work with (eager to learn, team-oriented, etc.). Practice until you feel positive and ready for real interviews!

Week 18: Job Search and Applications Strategy

Objectives (Week 18):
- Identify target roles: network engineer (entry-level), network administrator, NOC technician, IT support with networking focus, etc., ideally that list CCNA or similar as requirement.
- Use job boards (LinkedIn jobs, Indeed, Cisco's own, local companies' career pages) to find openings. Aim to apply to multiple jobs per week – job hunting can be a numbers game.
- Customize your cover letter (if requested) for each job – highlight how your skills match their environment (if they mention Cisco ASA, say you have strong Cisco knowledge and are learning firewalls, etc.). If no cover letter, your resume should have keywords matching their needs.
- Use your network: reach out to any contacts in the industry. Let them know you're CCNA certified and looking for roles. A referral can often get your resume seen.
- Consider joining professional communities: e.g., Cisco Learning Network, local networkers meetup, maybe user groups (even virtual). Sometimes job leads appear there.
- Prepare to discuss salary: research typical entry-level network engineer salary in your region. Have a range in mind (don't bring up unless asked, but be ready). With CCNA, you often have a bump over just general IT tech.
- Keep learning lightly: as you apply, perhaps peek at CCNP topics or SDN trends – not to dive deep but to show you're forward-thinking in interviews ("I plan to pursue CCNP next" or "I'm also exploring Python automation beyond CCNA"). This demonstrates initiative.
- Track your applications (perhaps in a spreadsheet or Trello) – company, role, date applied, status, so you can follow up if needed and prepare for each interview specifically (research each company's network or business, so you can tailor answers).
- Don't get discouraged by rejections or silence; it's part of the process. Use any feedback to improve. Celebrate small wins (like an HR screening call) as progress.

Resources:
- *Job postings:* Look at the requirements and responsibilities – note common themes (like maybe many want knowledge of OSPF, BGP (even if you only know basics of BGP), VLANs, etc.). Make sure those terms are on your resume if you have exposure (except don't lie if you truly never touched something).
- *Cisco Networking Academy Alumni network* – sometimes NetAcad has partnerships or job boards for alumni; check that out.
- *Mentor advice:* If you have a mentor or someone who's a network engineer, ask them to refer you or guide you on entry points (e.g., maybe start at an ISP NOC which often hires CCNAs for network monitoring – great learning environment).
- *Recruiters:* Talk to IT recruiters; some specialize in networking roles. They can also give resume tips or connect you with contract positions to get experience.

Milestones:
- **Milestone 1:** Apply to at least X jobs this week (X depends on availability, maybe 5-10 quality applications). Ensure each application you send has a tailored resume (if needed) and you follow any instructions (some have questionnaires – answer carefully).
- **Milestone 2:** Reach out to at least 3-5 professionals in networking – could be LinkedIn messages (e.g., "Hi, I just got my CCNA and am looking for entry opportunities; I admire your career path, any advice you might share would be greatly appreciated." – some might not reply, but some will and could offer

help). Also, don't hesitate to let friends know; sometimes opportunities come from casual connections.
- **Milestone 3:** Prepare a quick “elevator pitch” for networking events or introductions: “I recently became CCNA-certified and built extensive home lab projects; I’m excited to start a career in networking, particularly in network support or junior admin roles where I can further grow and contribute to a team.” This helps when speaking to recruiters or at job fairs.
- **Checkpoint:** The job search might take weeks or a few months, but you’ve set it in motion. Keep up momentum and while waiting for responses, continue light study or labbing to keep skills fresh (and reduce anxiety). Now, final week ahead, we’ll refine any last interview issues and plan continuous development.

Motivation: Job hunting can be a job in itself – treat it like part of your study plan. You are selling a product (your skills) that are genuinely valuable. Each “no” gets you closer to a “yes” statistically, and you only need one yes. Remember your worth with CCNA + your dedication – not everyone has the persistence to do what you did. Use that confidence when reaching out and interviewing. You are not begging for a job; you are offering to help employers with your fresh skills and enthusiasm. That positive, proactive mindset will shine through.

Week 19: Interview Refinement and Continuous Learning

Objectives (Week 19):
- By now you may start getting interview calls. This week, focus on any *specific feedback or upcoming interviews*. E.g., if you have an interview scheduled with a company that uses Cisco Meraki, read a bit about Meraki dashboard so you can mention it. If one interview revealed a gap (say you got stumped by a BGP question), do a quick study on BGP basics so you’re better prepared next time.
- Continue refining soft skills: practice speaking clearly about your experiences, maybe refine a story of how you tackled a learning challenge (e.g., your six-month study journey itself is a great story to show determination and how you handle a long-term project).
- Network further: maybe attend a local networking meetup or an online webinar Cisco hosts. Sometimes you can mention these in interviews (“Recently I joined a Cisco webinar on SD-WAN, I’m really interested in how that’s shaping networks” – shows interest beyond just what you had to study).
- Plan for **continued learning**: Many interviewers ask “What are your future plans?“. State that you intend to keep advancing – maybe plan CCNP Enterprise or DevNet Associate next, or that you’re curious about cloud networking (if that’s true). This signals you’ll grow with the role.
- If job offer comes in (woohoo!), analyze it: consider role duties and growth opportunity, not just salary. As an entry-level, you want a place where you can learn from senior engineers and get hands-on. If multiple offers, weigh pros/cons (maybe consult your mentor).
- Even after landing a job, schedule time for continuous improvement. But for now, let’s focus on acing any final interviews.

Resources:
- *Advanced topics glimpses:* If applying to places with more advanced tech (like BGP, NAT64, wireless controllers), you may not know deeply but a Cisco Live presentation or NetworkChuck video on that topic can give you talking points.
- *Community help:* The Cisco Learning Network forums have career sections – you can ask for advice or read others’ stories of getting first job.
- *Etiquette:* If you get offers or rejections, know how to professionally handle them (e.g., thank them for consideration even if rejected – sometimes they keep you in mind for future if you’re gracious).
- *Personal development:* Maybe pick up a book on professional soft skills or time management – this can indirectly improve your workplace readiness.

Milestones:
- **Milestone 1:** Evaluate how interviews are going. If you've done a few, what pattern of questions emerges? Are there any you consistently struggle with? Focus on those now intensely. Perhaps mock answer in front of a mirror until it's smooth.
- **Milestone 2:** If you have an upcoming technical assessment or second-round interview, prepare specifically: e.g., review that company's tech stack (maybe gleaned from job description) and be ready to discuss those topics. Also have some intelligent questions to ask them (like "I saw you use EIGRP – are you planning any migration to OSPF or BGP? What's the team's approach to new technologies?" – shows you care and think ahead).
- **Milestone 3:** Keep applying if needed. Aim to fill your pipeline – interviews often come in waves. The more you do, the more confident you become.
- **Checkpoint:** By end of Month 6, ideally you have landed a job or are in late stages. If not, don't despair – sometimes it takes longer. Keep up applications and maybe seek feedback from each interview to improve. Use the CCNA community for support. The key is not to stagnate: while searching, maybe start on CCNP ENCOR study or labs to stay sharp and become even more qualified. That could be integrated as next steps (though beyond this plan's scope).

Motivation: You've transformed from a beginner to a certified professional with a plan. That's huge! Now the challenge is to get someone to give you that break – and they will, because your preparation shows. Stay persistent and maintain the learning mindset. The end of this 6-month plan is really the beginning of your career journey. The habits you built – regular study, lab practice, note-taking – will serve you well on the job and for future certs. Be proud of how far you've come, and get excited for what's ahead. **You got this!**

CCNA 200-301 Exam Blueprint Topics Reference

(For quick lookup, all official exam topics are listed below – ensure you've covered each in the study plan above.)

- **1.0 Network Fundamentals:** Network components (Routers, Switches, Firewalls, APs, Controllers, Endpoints, Servers, PoE) [5]; Topology architectures (2-tier, 3-tier, spine-leaf, WAN, SOHO, cloud) [6]; Physical media (fiber vs copper, Ethernet modes) [7]; Interface/cable issues (collisions, errors, duplex/speed) [113]; TCP vs UDP [8]; IPv4 addressing and subnetting (incl. VLSM) [9]; Private vs public IPv4 [79]; IPv6 addressing and prefix (link-local, global, etc.) [114]; IPv6 address types (global unicast, unique local, link-local, anycast, multicast, EUI-64) [12] [13]; Client IP settings (verify on Windows, Mac, Linux) [83]; Wireless basics (nonoverlapping channels, SSID, RF, encryption types) [115] [116]; Virtualization fundamentals (servers, containers, VRFs) [85]; Switching concepts (MAC learning & aging, frame forwarding & flooding, MAC address table) [14].

- **2.0 Network Access:** VLANs (normal range) on multiple switches – access ports, default VLAN, inter-VLAN connectivity [87] [15]; Interswitch connectivity – trunking (802.1Q), native VLAN [16]; Layer 2 discovery protocols (CDP/LLDP) [17]; EtherChannel (LACP) configuration [18]; Spanning Tree Protocol (Rapid PVST+) – purpose and basic operations (root bridge, root port, port states, PortFast) [19] [20]; Cisco Wireless architectures & AP modes (e.g., autonomous, controller-based) [117]; Physical WLAN components and connections (WLC, APs, switches, management access like SSH/HTTPS) [118] [21]; WLC GUI for WLAN configuration (create WLAN, set security like WPA2, QoS, advanced settings) [119].

- **3.0 IP Connectivity:** Interpret routing table components (route source codes, prefix, network mask, next hop, AD, metric, gateway of last resort) [23] [24] [25]; Determine router forwarding decisions (longest prefix match, then AD, then metric) [25] [120]; Configure and verify IPv4 & IPv6 static routes (including default route, network route, host route, floating static) [26] [91]; Single-area OSPFv2 configuration & verification (neighbor adjacencies, network types like point-to-point vs broadcast DR/BDR, Router ID) [28] [29]; Purpose of first-hop redundancy protocols (HSRP, VRRP, GLBP) – concepts of virtual gateway for redundancy [30].

- **4.0 IP Services:** NAT (configure & verify **inside source NAT** – static mapping and NAT pool for PAT) [31]; NTP (configure & verify NTP client and NTP server mode) [32]; DHCP and DNS in network (DHCP provides IP config to clients; DNS resolves names to IPs) [96] [96]; SNMP in network operations (monitoring via SNMP gets/traps) [34]; Syslog (use of logging facilities and severity levels) [35]; Configure DHCP client and relay (e.g., `ip helper-address`) [36]; QoS concepts – QoS (Quality of Service) traffic prioritization (classification and marking, queuing, congestion management, policing, shaping) [37]; Configure device remote access via SSH (enable SSH server on Cisco device, e.g., generate RSA keys, set domain, use local AAA) [121] [39]; Functions of TFTP/FTP in network (file transfers for config/images, smaller vs larger file considerations) [122] [40].

- **5.0 Security Fundamentals:** Key security concepts (threats, vulnerabilities, exploits, mitigation techniques) [41]; Security program elements (user training, awareness, physical access controls) [42]; Device access control using local passwords (console, VTY, enable secret) [44]; Password policies (complexity, change schedule, multi-factor auth, certificate/bio alternatives) [45] [46]; Remote access vs site-to-site VPN definitions (VPN technology ensures secure communication over untrusted networks) [106]; Configure & verify access control lists (IPv4 ACLs – standard and extended – to filter traffic) [107] [50]; Layer 2 security features (DHCP snooping, Dynamic ARP Inspection, port security on switches – to prevent common L2 attacks) [52] [51]; Authentication, Authorization, Accounting (AAA) concepts (what each means, e.g., AAA server usage) [105]; Wireless security protocols (WEP, WPA, WPA2, WPA3 differences) [54]; Configure WLAN with WPA2 PSK via GUI (on WLC or wireless router) [56].

- **6.0 Automation & Programmability:** How automation impacts network management (e.g., simplifies repetitive tasks, reduces errors, allows scaling) [123]; Comparison of traditional networks vs controller-based (the latter centralizes control and uses automation, e.g., Cisco DNA Center) [124] [110]; Controller-based and software-defined architectures (overlay/underlay networks, fabric concepts, separation of control plane vs data plane, northbound and southbound APIs) [108] [58]; Compare traditional device management vs Cisco DNA Center (command-line per box vs centralized GUI/API with automation) [60]; REST-based APIs characteristics (CRUD operations mapping to HTTP verbs GET/POST/PUT/DELETE, uses JSON or XML payloads) [61] [62]; Configuration management tools capabilities (Puppet, Chef, Ansible – use templates/recipes to push configs, often with version control, automate provisioning) [63] [64]; Interpret JSON encoded data (understand key-value structure in JSON output or config data) [65] [66].

You've reached the end of the 6-month plan – equipped with knowledge, skills, and a roadmap for career success. Best of luck on your CCNA exam and the exciting networking career ahead!

[1] [70]

---

[1] [4] [67] [71] [111] [112] Passed CCNA 200-301. Recommended Study Materials and Tips. : r/ccna
https://www.reddit.com/r/ccna/comments/jgylcp/passed_ccna_200301_recommended_study_materials/

[2] [12] [13] [14] [41] [42] [51] [53] [55] [94] [95] [98] [99] [100] [101] [102] [103] Exclusive Cisco 200-301 CCNA Syllabus | Updated 2025
https://www.nwkings.com/cisco-ccna-syllabus

[3] [8] [9] [10] [11] [15] [16] [17] [18] [19] [20] [21] [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35] [36] [37] [38] [39] [40] [43] [44] [45] [46] [47] [48] [49] [50] [52] [54] [56] [57] [58] [59] [60] [61] [62] [63] [64] [65] [66] [79] [83] [84] [85] [87] [88] [89] [91] [96] [97] [105] [106] [107] [108] [109] [110] [114] [115] [116] [117] [118] [119] [120] [121] [122] [123] [124] CCNA 200-301 Syllabus 2026: All You Need to Know
https://www.theknowledgeacademy.com/blog/ccna-200-301-syllabus/

[5] [6] [7] [90] [113] Microsoft Word - 200-301-CCNA-v1.0 edited.docx
https://learningcontent.cisco.com/documents/200_301_CCNA_v1.0_2.pdf

[68] Share Your Top 3 CCNA Exam Study and Preparation Tips
https://learningnetwork.cisco.com/s/question/0D56e0000BzmFX7CQM/share-your-top-3-ccna-exam-study-and-preparation-tips

[69] [70] [72] [73] [76] [77] [80] [81] [92] [93] CCNA 200-301 Full Course | Jeremy's IT Lab
https://courses.jeremysitlab.com/p/ccna

[74] OSI Model Reference Chart - Cisco Learning Network
https://learningnetwork.cisco.com/s/article/osi-model-reference-chart

[75] Lab#1.1 - OSI model in practice | NetworkAcademy.IO
https://www.networkacademy.io/ccna/network-fundamentals/osi-model-in-practice

[78] 3.5.5 Packet Tracer – Investigate the TCP/IP and OSI Models in ...
https://itexamanswers.net/3-5-5-packet-tracer-investigate-the-tcp-ip-and-osi-models-in-action-answers.html

[82] 6 Different types of Network Topology Architectures
https://www.nwkings.com/types-of-network-topology-architectures

[86] The All-In-One OSI Model Cheat Sheet 2025 - StationX
https://www.stationx.net/osi-model-cheat-sheet/

[104] [PDF] Routing TCP/IP, Volume II (CCIE Professional Development)
https://elhacker.info/manuales/Redes/Cisco/Routing/Routing%20TCP%20IP%20Volume%202.pdf